Clarifications for queries received for tender enquiry no. BESCOM/2025-26/SE0441

Sl. No	Tender Document Clause/Page No.	Clause as per tender document	Clarification/Amendment/ Addendum sought by prospective Bidders	BESCOM Clarification
1	Pre-Qualification requirement stipulated under Section 1, Sl. No. 2	a.) The Bidder should have experience of providing and/or implementing at least one On-Premises Cyber Security Operations Center (C-SOC) services which includes NG SIEM, SOAR and UEBA for any State Government / Central Government / PSU in India during the last five financial years (2020–21, 2021–22, 2022–23, 2023–24 & 2024–25) b) Cost of any 1 such project said in point (a) shall not be less than 50% (Rs. 15 Crores) of estimated value of contract. Note: Updated to the FY in which the tenders are invited. The value of the completed works shall be given a weightage of 10% per year to bring them to the price level of FY in which the tenders are invited.	In view of the foregoing, it is respectfully requested that the eligibility criteria may kindly be reviewed and suitably revised to require experience in the implementation of C-SOC with SIEM, which has been prominently and widely deployed across Government and PSU organizations throughout India.	Tender Conditions Prevails. -No changes
2			To please amend this clause as: The Bidder should have the experience of providing and/or implementing at least One On premises Cyber Security Operations Center (C-SOC) services which includes NGSIEM/SOAR/UEBA/Cyber Security Component/Data Center Component for any State government /Central Government/PSU in India during the last Seven Financial Years.	Tender conditions prevail. - No change
3			Change Request - a) The Bidder should have the experience of providing and/or implementing Any 4 items of below, at least One On premises Cyber Security Operations	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:29:49 +05'30'

			Center (C-SOC) services which includes NGSIEM/ SOAR /NBAD/ UEBA /DAM/TIP/ NAC/ EDR/VM/ EASM/ WAF/ UEM/ NGFW (Internal)/NGFW (External)/ WIPS/PIM-PAM for any State government /Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25). - b) Cost of any 1 such project said in point (a) shall not be less than 50% (Rs. 15 Crores) of estimated value of contract. Note: Updated to the FY in which the tenders are invited. The value of the completed works shall be given a weightage of 10% per year to bring them to the price level of FY in which the tenders are invited.	
4			This approach enables the platform to be delivered through a unified single console, ensuring seamless integration between SIEM, SOAR, UEBA & NBAD/ NDR components from the same OEM. Also it results in more accurate threat detection, faster 1automated response, reduced false positives, and eliminates	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:31:58 +05'30'

			visibility gaps that commonly arise when using soiled security tools from multiple vendors. Additionally, this requirement will encourage participation from OEMs with extensive experience in delivering unified security platforms, thereby ensuring a more mature, reliable, and well-integrated solution for the customer.	
5			The Bidder/OEM should have the experience of providing and/or implementing at least One On premises Cyber Security Operations Center (C-SOC) services which includes NGSIEM, SOAR and UEBA for any State government /Central Government/PSU/Private in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25).	Tender conditions prevail. - No change
6			All the proposed solutions (SIEM, SOAR, UEBA, NBAD/NDR) should be deployed for any State government/Central Government/PSU/Private in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:31:37 +05'30'

			25)., supported with PO/Work order/Invoice copy	
7			The proposed NBAD/NDR solution should have been successfully implemented for any State government/Central Government/PSU/Private in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25).supported with PO/Work order/Invoice copy	Tender conditions prevail. - No change
8			Request to amend the clause as: a) The Bidder should have the experience of providing and/or implementing at least One On-premises Cyber Security Operations Center(C-SOC) services which includes NG-SIEM, SOAR and UEBA for any State government /Central Government/PSU in India during the last Five Financial Years(2020-21, 2021-22, 2022-23, 2023-24 & 2024-25). b) Cost of any 1 such project said in point (a) shall not be less than (Rs. 5 Crores) and Cost of 2 projects cumulatively should be not less than not be less than 50% (Rs. 15 Crores) of estimated value of contract.	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:34:30 +05'30'

			Note: Updated to the FY in which the tenders are invited. The value of the completed works shall be given a weightage of 10% per year to bring them to the price level of FY in which the tenders are invited.	
9			Request to amend the clause as: All the proposed solutions (SIEM, SOAR, UEBA, NBAD/NDR) should be deployed for any State government/Central Government/PSU/Public Limited in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25)., supported with PO/Work order/Invoice copy	Tender conditions prevail. - No change
10			Change request: a) The Bidder or OEM should have the experience of providing and/or implementing at least One On-premises Cyber Security Operations Center (C-SOC) services which includes NGSIEM, SOAR and UEBA for any State government /Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25).	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:34:43 +05'30'

			Justification: The SOC and related technologies are latest and the experience will be by the OEM and OEMs are going to be the key stake holders who will handhold and train and train the Bidders to execute the project successfully. Hence, we request BESCOM to consider the Bidder or OEM experience for the clause mentioned in the tender.	
11			Change request: a) The Bidder or OEM should have the experience of providing and/or implementing at least One On premises Cyber Security Operations Centre (C-SOC) services which includes NGSIEM. SOAR and UEBA for any State government/Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25). Justification: The SOC and related technologies are latest, and the experience will be by the OEM and OEMs are going to be the key stake holders who will handhold and train the Bidders	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:34:56 +05'30'

			to execute the project successfully. Hence we request BESCOM to consider the Bidder or OEM experience for the clause mentioned in the tender.	
12			The SOC and related technologies are latest, and the experience will be by the OEM and OEMs are going to be the key stake holders who will handhold and train and train the Bidders to execute the project successfully. Hence we request BESCOM to consider the Bidder or OEM experience for the clause mentioned in the tender.	Tender conditions prevail. - No change
13			a. The Bidder should have the experience of providing and/or implementing Any 4 items of below, at least One On Premises Cyber Security Operations Center (C-SOC) services which includes NGSIEM/ SOAR /NBAD/ UEBA /DAM/TIP/ NAC/ EDR/VM/ EASM/ WAF/ UEM/ NGFW (Internal)/NGFW (External)/ WIPS/PIM-PAM for any State government /Central Government/PSU in India during the last Five Financial Years (2020-21,2021-22,2022-	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:35:11 +05'30'

			23,2023-24 and 2024-25). b. Cost of any 1 such project said in point (a) shall not be less than 50percentage (Rs.15 Crores) of estimated value of contract. Note. Updated to the FY in which the tenders are invited. The value of the completed works shall be given a weightage of 10 percentage per year to bring them to the price level of FY in which the tenders are invited.	
14			Request BESCOM to amend the clause as All the proposed solutions SIEM, SOAR, UEBA, NBAD NDR should be deployed by OEM BIDDER for any State government Central Government PSU BFSI Enterprise in India during the last Five Financial Years 2020 21 2021 22 2022-23, 2023-24, 2024- 25 and 2025-26) and till up to the last date of tender Submission , supported with PO/Work order/Invoice copy.	Tender conditions prevail. - No change
15			Request BESCOM to amend the clause as Experience The bidder should have the experience of providing and/or implementing at least One On-premises Cyber Security Operations Center CSOC services which includes	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:35:24 +05'30'

			NG-SIEM, SOAR and UEBA for any State government/Central Government PSU BFSI Enterprise in India during the last Five Financial Years 2020 21, 2021-22, 2022-23, 2023-24, 2024- 25 and 2025-26) and till up to the last date of tender Submission.	
16			Since this project is covering SOC SIEM SOAR UEBA along with other Technologies like EDR DAM NDR Cloud WAAP RASP Unified Endpoint Management etc., Request BESCOM to reconsider Cyber Security Products and Service Request the clause to be amended as a The Bidder should have the experience of providing and or implementing at least One On premises Cyber Security Operations Center CSOC services which includes NGSIEM SOAR and UEBA Cyber Security Solutions and or Services for any State government Central Government PSU BFSI Enterprise in India during the last Five Financial Years and till the last date of bid submission 2020 21 2021 22 2022 23 2023 24 2024 25 2025 26	Tender conditions prevail. - No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:35:38 +05'30'

			b The cost of a single project, or the cumulative value of multiple projects as specified in clause a shall not be less than 50 percent Rupees15 Crores) of the estimated contract value. For the purpose of evaluation, the value of completed works shall be updated to the price level of the Financial Year in which tenders are invited by applying a 10 percent weightage per annum	
17	Pre-Qualification Requirements Page No 4	Declaration from Directors of the Company in MBP-1 Form, stating that they are not disqualified to be a Director of the Company, along with the list of Companies in which they are Directors as on the date of inviting tender (s).	Please Clarify	Declaration from Directors of the Company in MBP-1 Form, stating that they are not disqualified to be a Director of the Company, along with the list of Companies in which they are Directors as on the date of inviting tender (s).Self declaration to be submitted by Directors as per Company's Act.
18	Page No 10; Technical Scoring criteria	Experience: The bidder should have the experience of providing and/or implementing at least One On-premises Cyber Security Operations Center (C-SOC) services which includes NG-SIEM, SOAR and UEBA for any State government/Central Government/PSU in India	For Wider Participation we request tender inviting authority to please amend this clause as: The bidder should have the experience of providing and/or implementing at least One On-premises Cyber Security Operations Center (C-SOC) services which includes NG-SIEM/SOAR/UEBA/Cyber	Tender conditions prevail – No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:35:52 +05'30'

		during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25).	Security Component/Data Center Component for any State government/Central Government/PSU in India during the last Seven Financial Years. No of Projects completed □ =1 - 5 Points □ >1 - 10 Points	
19			a)The Bidder should have the experience of providing and/or implementing Any 4 items of below, at least One On premises Cyber Security Operations Centre (C-SOC) services which includes NGSIEM/ SOAR /NBAD/ UEBA /DAM/ TIP/NAC /EDR /VM/ EASM/ WAF/ UEM/ NGFW (Internal)/NGFW (External)/ WIPS/PIM-PAM for any State government /Central Government/PSU in India during the last Five Financial Years (2020-21,2021-22,2022-23,2023-24 &2024-25). b) Cost of any 1 such project said in point (a) shall not be less than 50percentage (Rs. 15 Crores) of estimated value of contract. Note Updated to the FY in which the tenders are invited. The value of the completed works shall be given a weightage of	Tender conditions prevail – No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:36:08 +05'30'

			10percentage per year to bring them to the price level of FY in which the tenders are invited. Value of Projects completed equal to 30 Cr - 5 Points greater than 30Cr-10 Points	
20	Page No 10; Technical Scoring criteria	The bidder should have IT Security professionals on its pay rolls who should be CEH/CISSP/CISA/ CISM/ CCNA/CCNP Certified. Attach supporting documents. Number of IT Professionals: □ 10 to 15- 7 Points □ 15 or more - 10 Points	For Wider Particiaption we request tender inviting authority to please ammend this clause as: The bidder should have IT Security professionals on its pay rolls who should be CEH/CISSP/CISA/ CISM/ CCNA/CCNP Certified. Attach supporting documents. Number of IT Professionals: □ 5 to 10- 7 Points □ 10 or more - 10 Points	Tender conditions prevail – No change
21	Proof of Concept Demonstration Bidder to demonstrate the following features of the proposed tools /solution / platform to the committee appointed by BESCOM Pg no 15	The Bidder shall have implemented the proposed ITSM solution in at least one Government / PSU / utility organization during the last 05 years.	To ensures the solution is proven at scale within Government/PSU environments, reducing implementation risk and ensuring domain maturity, regulatory alignment, and operational stability. It safeguards BESCOM's interests by mandating demonstrated success across multiple similar public-sector deployments. hence	Tender conditions prevail. -No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:36:22 +05'30'

			We request you to change the clause as per the following "The proposed ITSM should be implemented in at least 5 Government / PSU / utility organization during the last 05 years."	
22	Proof of Concept Demonstration Bidder to demonstrate the following features of the proposed tools /solution / platform to the committee appointed by BESCOM Pg no 15	additional clause for POC/ITSM ticketing tool	Adding the following clause in the RFP requiring ITIL alignment and ITIL4 certification justifies the adoption of best practices, quality assurance, and standardized IT service management. It ensures improved efficiency and vendor expertise while setting clear expectations and demonstrating a commitment to continuous improvement in IT practices.	Tender conditions prevail. -No change

23	Proof of Concept Demonstration: External Attack Surface Monitoring Page no 15	Ability to detect, monitor and shutdown all kinds of incidents given below: Phishing, Pharming, Brand Abuse, rouge websites and mobile apps related to BESCOM, Email address used for fraudulent purpose. Detection Mechanisms to track usage of BESCOM digital watermark, Real-time monitoring of web-server referrer logs. Track new domain	The POC points to demonstrated are not the technical specifications of EASM. And moreover the features requested to demonstrate is Brand monitoring solution rather than external attack surface management. We hereby request you to change them with below points:	Tender Conditions Prevail. -No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:36:36 +05'30'

		name registrations to detect any spoofed site being registered. Monitor & report abuse mailbox provided to customers	* Should be able to provide the internal device asset's latest risk score, OS, IP address, last user, vulnerabilities, discovery source and when the device was first and last seen. * Provide risk assessment for each device asset and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events and risk level for each discovered risk.	
24	Page no 11 Clause 6	The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large scale high demand environments for future expansions as well supported with PO Work order Invoice copy.	The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setup in any one Indian Critical Government Organization with 25000 EPS in the last 5 years supported with PO Work Order Invoice copy. Since this requirement relates to the product capability and deployment credentials of the OEM solution manufacturer rather than the system integrator service provider we request clarification that this eligibility may be considered under the OEM experience and not mandatorily under the bidder credentials. Accordingly we request the authority to kindly	Tender Conditions prevail. -No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:36:51 +05'30'

			confirm acceptance of OEM credentials and documentary proof for compliance to this clause	
25	Page no 11 Clause 6	The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large scale high demand Environments for future expansions as well supported with PO Work order Invoice copy.	We understand that the clause states The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setup in any one Indian Critical Government Organization with 25000 EPS in the last 5 years supported with PO Work Order Invoice copy Considering long term managed security service engagements and lifecycle based operations we request the authority to kindly modify the clause to include deployments which are implemented or currently managed during the last 10 years and also allow experience of bidder subsidiary group companies in addition to the bidder Accordingly we request the clause to be revised to allow implemented or managed projects during the last 10 years including experience of bidder or its subsidiary supported with documentary proof	Tender Conditions prevail. -No change
			We understand that the clause states The proposed NG SIEM	Tender Conditions prevail. -No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:37:05 +05'30'

26			solution should have been successfully supplied and implemented in an on premise setup in any one Indian Critical Government Organization with 25000 EPS in the last 5 years supported with PO Work Order Invoice copy Considering long term managed security service engagements and lifecycle based operations we request the authority to kindly modify the clause to include deployments which are implemented or currently managed during the last 10 years and also allow experience of bidder subsidiary group companies in addition to the bidder Accordingly we request the clause to be revised to allow implemented or managed projects during the last 10 years including experience of bidder or its subsidiary supported with documentary proof	
27	Pre-Qualification Requirements Page no 6	4. The Bidder or his OEM shall have a) ISO 9001:2015 or latest certification. b) ISO 27001:2022 or latest certification	Request to amend the clause as: 4. The Bidder or his OEM shall have a) ISO 9001:2015 / TL 9000 or latest certification. b) ISO 27001:2022 or latest certification	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:37:19 +05'30'

28			Change request: Bidder or his OEM shall be an empanelled cyber security firm by CERT-In/MeitY. Justification: However, to ensure the holistic security of the infrastructure and to validate the practical implementation capabilities of the bidder or OEM, as it is vital to possess the MeiTY Certification.	Tender Conditions Prevail. -No Change
29			We respectfully request the removal of the CERT In Empanelment requirement for this scope. CERT In empanelment is specifically designed to vet organizations for Auditing, Vulnerability Assessment VAPT and Forensic services In contrast, the provision of Cyber Security Products and Managed SOC services relies on operational frameworks such as ISO 27001 and product efficacy. Applying an auditing credential to a product-based contract unnecessarily restricts the pool of qualified bidders without adding relevant technical oversight	Tender Conditions Prevail. -No Change
30	Technical Scoring criteria: Page no 10	4. The proposed NBAD/NDR solution should have been successfully implemented for	Request to amend the clause as: 4. The proposed NBAD/NDR solution should have been	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:37:35 +05'30'

		any State government/ Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22,2022-23, 2023-24 & 2024-25) supported with PO/Work order/Invoice copy	successfully implemented/managed for any State government/Central Government/PSU/Public Limited in India during the last Five Financial Years (2020-21, 2021-22,2022-23, 2023-24 & 2024-25) supported with PO/Work order/Invoice copy	
31			Request BESCOM to Amend the Clause as The proposed NBAD NDR solution should have been successfully implemented by OEM/Bidder for any State government/Central Government/PSU/BFSI Enterprise in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24, 2024 25 and 2025 26 and till up to the last date of tender Submission. Supported with PO/Work order/Invoice copy	Tender Conditions Prevail. -No Change
32			Bidder or OEM should have successfully implemented proposed NBAD/NDR solution for any State government/Central Government/PSU in India during the last Five Financial Years (2020-21,2021-22,2022-23,2023-24 &2024-25). supported with PO/Work	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:37:52 +05'30'

			order/Invoice copy Number of Implementations by Bidder/OEM Less than 1-0 Points and 1 to 2-7 Points and 2 or more-10 Points	
33	Technical Scoring criteria: Page no 11	6. The proposed NG-SIEM solution should have been successfully supplied and implemented in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large-scale high-demand environments for future expansions as well, supported with PO/Work order/Invoice copy. Supply Experience- Number of references with Events Per Second(EPS): □ No References – 0 Points □ = 1 References– 8 Points □ >= 2 References–10 Points	Request to amend the clause as: 6. The proposed NG-SIEM solution should have been successfully supplied and implemented/Implementing in an on premise setup/managed setup in any one Indian Critical Government Organizations/ PSU/ BFSI/ Government/Public Limited with 25000 EPS in the last 5 years considering the capability to support large-scale high- demand environments for future expansions as well, supported with PO/Work order/Invoice copy. Supply Experience- Number of references with Events Per Second(EPS): □ No References – 0 Points □ = 1 References– 15 Points □ >= 2 References–30 Points	Tender Conditions Prevail. -No Change
34			The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setup in any one Indian Critical Government	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:38:08 +05'30'

			Organization with 25000 EPS in the last 5 years supported with PO Work Order Invoice copy. Since this requirement relates to the product capability and deployment credentials of the OEM solution manufacturer rather than the system integrator service provider we request clarification that this eligibility may be considered under the OEM experience and not mandatorily under the bidder credentials. Accordingly we request the authority to kindly confirm acceptance of OEM credentials and documentary proof for compliance to this clause	
35	Page 11 Technical Scoring criteria clause 6	The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large scale high demand environments for future expansions as well supported	We understand that the clause states The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setup in any one Indian Critical Government Organization with 25000 EPS in the last 5 years supported with PO Work Order Invoice copy Considering long term managed security service engagements and lifecycle based operations we request the authority to kindly modify the	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:38:25 +05'30'

		with PO Work order Invoice copy.	clause to include deployments which are implemented or currently managed during the last 10 years and also allow experience of bidder subsidiary group companies in addition to the bidder Accordingly we request the clause to be revised to allow implemented or managed projects during the last 10 years including experience of bidder or its subsidiary supported with documentary proof	
36			The proposed NG SIEM solution should have been successfully supplied and implemented in an on premise setup in any one Indian Critical Government Organization with 25000 EPS in the last 5 years supported with PO Work Order Invoice copy. Since this requirement relates to the product capability and deployment credentials of the OEM solution manufacturer rather than the system integrator service provider we request clarification that this eligibility may be considered under the OEM experience and not mandatorily under the bidder credentials. Accordingly	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:38:41 +05'30'

			we request the authority to kindly confirm acceptance of OEM credentials and documentary proof for compliance to this clause	
37			Request BESCOM to amend the clause as The proposed NG SIEM solution should have been successfully supplied and implemented by OEM Bidder in an on-premise setups in any one Indian Critical Government Organizations/PSU/Govt/BFSI/ Enterprise with 7500 EPS in the last 5 years (2020-21, 2021-22, 2022-23, 2023-24, 2024- 25 and 2025-26) and till up to the last date of tender Submission. supported with PO/Work order/Invoice copy	Tender Conditions Prevail. -No Change.
38			Bidder/OEM should have successfully supplied and implemented the proposed NG-SIEM solution in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large-scale high demand environments for future expansions as well, supported with PO/Work order/Invoice copy.	Tender Conditions Prevail. -No Change.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:38:59 +05'30'

39	PgNo13	POC Criteria Request you to kindly Define limited integration.	Can The POC demonstrated from the Bidders OEMs Lab.	Tender Conditions Prevail. -No Change
40	page no 10	All the proposed solutions (SIEM,SOAR,UEBA,NBAD/NDR) should be deployed for any State government/Central Government/PSU in India during the last Five Financial Years(2020-21,2021-22,2022-23,2023-24 and 2024-25).supported with PO/Work order/Invoice copy. Deployed in a single Government Organization-Less than three out of SIEM, SOAR, UEBA,NBAD-0 Points. Any three out of SIEM,SOAR,UEBA,NBAD-6 Points All the proposed solutions (SIEM,SOAR,UEBA,NBAD) 10 Points	All the proposed solutions (NGSIEM/SOAR/NBAD/UEBA/ DAM/TIP/NAC/EDR/VM/EASM /WAF/UEM/NGFW (Internal)/NGFW (External)/ WIPS/PIM-PAM) should be deployed for any State government/Central Government/PSU in India during the last Five Financial Years (2020-21, 2021-22, 2022-23, 2023-24 & 2024-25). supported with PO/Work order/Invoice copy. Deployed in a single Government Organization. Less than three out of NGSIEM/SOAR/NBAD/UEBA/DAM/TIP/NAC/EDR/VM/EASM/ WAF/UEM/NGFW (Internal)/NGFW(External)/ WIPS/PIM-PAM-0 Points. Any three out of NGSIEM/SOAR/NBAD/UEBA/DAM/TIP/NAC/EDR/VM/ EASM/ WAF/ UEM/NGFW (Internal)/NGFW (External)/WIPS/PIM-PAM-6 Points. All the proposed solutions (NGSIEM/SOAR	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:39:16 +05'30'

			/NBAD/UEBA/DAM/TIP/NAC/ EDR/VM/EASM/WAF/UEM/NG FW (Internal)/NGFW (External)/ WIPS/PIM-PAM)-10 Points	
41	Technical Scoring criteria: Page no.12	10) IR (Incident Response) Services offered as a part of Contract from OEM	Kindly clarify whether you are looking for a dedicated "IR as a service", in addition to the solutions. If that is the case, kindly share more details regarding the same.	Tender Conditions Prevails. -No changes.
42	Proof of Concept Demonstration: External Attack Surface Monitoring Page no 15	Ability to detect, monitor and shutdown all kinds of incidents given below: Phishing, Pharming, Brand Abuse, rouge websites and mobile apps related to BESCOM, Email address used for fraudulent purpose. Detection Mechanisms to track usage of BESCOM digital watermark, Real-time monitoring of web-server referrer logs. Track new domain name registrations to detect any spoofed site being registered. Monitor & report abuse mailbox provided to customers	The POC points to demonstrated are not the technical specifications of EASM. And moreover the features requested to demonstrate is Brand monitoring solution rather than external attack surface management. We hereby request you to change them with below points: * Should be able to provide the internal device asset's latest risk score, OS, IP address, last user, vulnerabilities, discovery source and when the device was first and last seen. * Provide risk assessment for each device asset and assign a risk score that can be monitored over time. Display risk indicators	Tender Conditions Prevail. -No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:39:33 +05'30'

			like what type of risks, events and risk level for each discovered risk.	
43	15 and External attack	Ability to detect, monitor and shutdown all kinds of incidents given below Phishing, Pharming, Brand Abuse, rouge websites and mobile apps related to BESCOM, Email address used for fraudulent purpose	The current Points of Demonstration outlined are not aligned with the technical specifications of External Attack Surface Management. In addition, the features requested for demonstration appear to relate more to a Brand Monitoring solution rather than EASM capabilities.	Tender Conditions Prevails. -No changes.
44	Page No 15	Threat Intelligence Platform	Can The POC demonstrated from the Bidders/OEMs Lab.	Tender Conditions Prevails. No changes.
45	Pg No 15	Proof of Concept Demonstration - Deception solution	Can The POC demostrated from the Bidders/OEMs Lab.	Tender Conditions Prevails. No changes.
46	PgNo 15	Proof of Concept Demonstration External Attack Surface Monitoring - External Attack Surface Monitoring	Can The POC demostrated from the Bidders/OEMs Lab.	Tender Conditions Prevails. No changes.
47	PgNo 15	Proof of Concept Demonstration - Ticketing Tool	Proof of Concept Demonstration - Ticketing Tool	Tender Conditions Prevails. No changes.
48	PgNo 14	SOAR	Can The POC demostrated from the Bidders/OEMs Lab.	Tender Conditions Prevails. No changes.
49	PgNo 10	All the proposed solutions SIEM SOAR UEBA NBAD NDR should be deployed for any State government Central Government PSU in India during the last Five Financial Years (2020 21 2021 22 2022	Request BESCOM to amend the clause as All the proposed solutions SIEM, SOAR, UEBA, NBAD NDR should be deployed by OEM BIDDER for any State government Central Government PSU BFSI Enterprise in India during the last Five Financial	Tender Conditions Prevails. No changes.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:39:51 +05'30'

		23 2023 24 2024 25 supported with POWork order Invoice copy	Years 2020 21 2021 22 2022-23, 2023-24, 2024- 25 and 2025-26) and till up to the last date of tender Submission , supported with PO/Work order/Invoice copy.	
50	PgNo 13	NG SIEM instance support Integration for minimum	This can be provided as the reference but would be challenging to set up the infrastructure for 25000 EPS.	Tender Conditions Prevails. No changes.
51	PgNo13	NBAD	Can The POC demostrated from the Bidders/OEMs Lab.	Tender Conditions Prevails. No changes.
52	PgNo 14	UEBA	Can The POC demostrated from the Bidders/OEMs Lab.	Tender Conditions Prevails. No changes.

53	Page 124 and 125 of Tender Document	On-Prem solution will be a very costly affair. We usually don't offer an on-prem solution for scope less than 10K assets. We would like to raise the query regarding the sbame to kindly consider subscription to our shared cloud platform. Also please specify how many number of assets to be scanned?	We would like to raise the query regarding the same to kindly consider subscription to our shared cloud platform. Also please specify how many number of assets to be scanned?	Tender conditions prevails - No changes. For number of assets to be scanned - Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:40:08 +05'30'

54	Page No. 127, Clause No.7	Spec as per RFP - SIEM solution must apply intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions using Agentic AI and GEN AI	The solution must apply intelligent analytics and threat intelligence to vast amount of security data to provide actionable insights into critical threats, enabling faster and more effective triage and response decisions, with advanced AI/ML capabilities. Kindly amend the clause to allow intelligent analytics and threat intelligence–driven investigation within the SIEM, with AI/ML capabilities provided through integrated solutions.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:40:25 +05'30'

55	Page No. 129, Clause No.29	Spec as per RFP -Solution must be capable of providing real time and on demand access to data sources such as evolving format, Custom API's, interfaced incl. text, XML, JSON, Data Base connections, Network Ports, Connections or from log data., and files	The solution must be capable of providing real-time and on-demand access to data ingested from a wide variety of sources, including logs, files, databases, network ports, APIs, and evolving data formats such as text, XML, and JSON, using OOTB supported connectors or inbuilt parsing mechanisms. ArcSight SIEM supports real-time and on-demand access to security data by ingesting information from diverse sources using Smart Connectors, Flex Connectors, and APIs supporting formats such as text, XML, and JSON, and supports databases, files, logs, and network ports (e.g., Syslog).	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:40:42 +05'30'

56	Page No. 130, Clause No.45	Spec as per RFP -The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability for security alert in Window Unix and Linux environment. to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment.	The cyber security solutions will not have performance monitoring tools, performance monitoring of Applications / Infrastructure needs to be separated. Hence to be deleted. The project is for Security operations, no security product in the world will have infrastructure/ applications performance monitoring tool.	Tender Conditions Prevail. No Change
57	Page No. 131, Clause No.64	Spec as per RFP - The solution should have the capability to add as many fields/columns in the index. The solution should support any number of fields in a particular row of data and should be able to store any amount of data in a particular field	The solution should support extensible event schemas, allowing addition of custom fields and columns as required. The solution should support a large number of fields per event and flexible field sizes within supported limits. Mention the Number of Field, columns and field data size should be defined to a permissible limit and cannot be infinite.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:40:59 +05'30'

58	Page No. 136, Clause No.20	Spec as per RFP - Solution should be capable of implementing a new integration without any coding requirment and should support no code based implementation.	Solution should be capable of implementing a new integration using no code/ Low Code based implementation. Any integration will require API's to be written with out which integration will be difficult, hence Low code to be allowed.	Tender Conditions Prevail. No Change
59	Page No. 136, Clause No.26	Spec as per RFP - Solution should track all forensic data related to an incident in one location (s system images, snapshots etc) and view the history of evidence across the entire incident	The solution should centrally track and manage all forensic data and evidence related to an incident, including logs, artifacts, files, and references to forensic outputs (such as system images or snapshots), and maintain visibility into the evidence history across the incident lifecycle. Forensic related artefacts can be part of Ticketing tool and needs to be added there.	Tender Conditions Prevail. No Change
60	Page No. 137, Clause No.57	Spec as per RFP - Solution should be able to identify coverage gaps by identifying missing mandatory controls in the environment.	Kindly elaborate on the use case requirement, as the gaps are covered in ITSM and not in CSOC services.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:41:16 +05'30'

61	SIEM; Suggested Clause	SIEM solution should be licensed based on standard licensing parameter (i. e. sustained events per second) and should be perpetual. Licenses should be considered for non-production sites (DR, UAT, DEV, TESTING) to benefit customer without any surplus license cost during the tenure of the project.	As per industry standard and the department will save license cost due to license applicable only to production server.	Tender Conditions Prevail. No Change
62	SIEM; Suggested Clause	SIEM and Prevention Security solutions like F/W, Packet Capture, IPS, HIPS, AV, DLP, NDR, EDR, NBAD, Router, Switches etc should be from different OEM. So that it can detect threats missed by other existing tools using the security defence in depth strategy.	As per industry standard and the department will save license cost due to license applicable only to production server.	Tender Conditions Prevail. No Change
63	SIEM; Suggested Clause	Quoted SIEM Solution must have its presence in India for more than 15 years and must have at least 3 deployments for more than 30000 EPS in Government of India organization. At least 3 sign-off must be attached for more than 30K EPS from Government of India organization. Customer Signoff need to be provided at the time of bidding.	As per industry standard and the department will save license cost due to license applicable only to production server.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:41:45 +05'30'

64	SOAR; Suggested Clause	SOAR capabilities within SIEM must not require any separate license and with no restriction on number of analysts. In case SOAR is not native or from different OEM, License should be proposed for 18 analysts.	As per industry standard and the department will save license cost due to license applicable only to production server.	Tender Conditions Prevail. No Change
65	Section 7 page 216	Supply & Procurement of Hardware - Part-A, Part-B, Part-C -55 percent	Supply & Procurement of Hardware - Part-A, Part-B, Part-C -70 percent	Tender Conditions Prevail. No Change
66	Section 7 page 216	Installation, Commissioning & SOC Control Room Setup - Part-B, Part-C, Part D (Licensing charges as per BoQ) - 25%	Installation, Commissioning & SOC Control Room Setup - Part-B, Part-C, Part D (Licensing charges as per BoQ) - 20%	Tender Conditions Prevail. No Change
67	Section 7 page 216	Factory Acceptance Test (FAT) User Acceptance Test (UAT) Post Implementation & SLA Compliance - Part-A, Part-B, Part-C - 20%	Factory Acceptance Test (FAT) User Acceptance Test (UAT) Post Implementation & SLA Compliance - Part-A, Part-B, Part-C - 10%	Tender Conditions Prevail. No Change
68	Section 7 page 217	Payment for subscription - Will be paid annually	Payment for subscription - We understand this is annual advance	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:42:33 +05'30'

69	4.4 Deployment of Security Tools and Technologies: e) Database Activity Monitoring (DAM); Page No. 55	Number of databases to be monitored	Please provide total database count and types (Oracle, SQL Server, MySQL, PostgreSQL, etc.)	Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document
70	4.4 Deployment of Security Tools and Technologies: e) Database Activity Monitoring (DAM); Page No. 55	Database deployment environment	Clarify on-prem vs cloud deployment, and total number of database servers/instances	Please refer the note mentioned below in this document
71	4.4 Deployment of Security Tools and Technologies: e) Database Activity Monitoring (DAM); Page No. 55	Transaction volume	Approximate daily transaction volume (TPS) and log volume (GB/day) for sizing purposes	Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:43:08 +05'30'

72	4.4 Deployment of Security Tools and Technologies: e) Database Activity Monitoring (DAM); Page No. 55	Privileged accounts	Number of DBA and service accounts to be monitored	Tender Conditions Prevail. No Change
73	4.4 Deployment of Security Tools and Technologies: e) Database Activity Monitoring (DAM); Page No. 55	Licensing metric	Confirm licensing metric: per DB server, per core, per instance, or per appliance	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
74	4.4 Deployment of Security Tools and Technologies: e) Database Activity Monitoring (DAM); Page No. 55	Retention & storage	Expected log retention period and storage sizing requirements	Please refer Section 5. Detailed Scope of Work, Clause 17 in page no. 84 of the tender documents.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:43:34 +05'30'

75	4.4 Deployment of Security Tools and Technologies: e) Database Activity Monitoring (DAM);; Page No. 55-56	High Availability / DR	Confirm if HA / clustering / DR setup is required	Please refer the note mentioned below in this document
76	4.4 Deployment of Security Tools and Technologies: h) RASP Mobile Application Security; Page No: 55-56	Applications to protect	Total number of mobile applications (Android/iOS) including production, UAT, and dev apps	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
77	4.4 Deployment of Security Tools and Technologies: h) RASP Mobile Application Security; Page No. 55-56	User base	Average monthly active users and expected annual downloads for sizing and license estimation	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
78	4.4 Deployment of Security Tools and Technologies: h) RASP Mobile Application Security; Page No. 55-56	Licensing model	Confirm licensing metric: per app, per MAU, per API call, or per year subscription	Please refer Section C. Tool AMC in Page no.221of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:43:58 +05'30'

79	4.4 Deployment of Security Tools and Technologies: h) RASP Mobile Application Security; ; Page No. 55-56	API coverage	Clarify whether backend API protection is included within RASP licensing	It is clarified that API protection is included within RASP licensing .
80	4.4 Deployment of Security Tools and Technologies: h) RASP Mobile Application Security; ; Page No. 55-56	Dashboard & hosting	Clarify whether monitoring dashboard is SaaS or on-prem, and data residency requirements	Please refer Clause 18.1 in Page 87 of the Tender Document.
81	4.4 Deployment of Security Tools and Technologies: h) RASP Mobile Application Security; ; Page No. 55-56	SOC integration	Method of alert forwarding to SOC (Syslog/API) and SLA for threat alerting	Please refer Clause 18 in Page 87 & 88 of the Tender Document.
82	4.4 Deployment of Security Tools and Technologies m) Unified Endpoint Management; Page 56-57	Device inventory	Total desktops, laptops, mac OS, Linux, Android, and iOS devices to be on boarded	Please refer Section C, Point 2.1 in Page 221 same count as EDR of the Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:44:24 +05'30'

83	4.4 Deployment of Security Tools and Technologies m) Unified Endpoint Management; Page 56-57	Device ownership	BYOD vs corporate-owned split and remote workforce percentage	Tender Conditions Prevail. No Change
84	4.4 Deployment of Security Tools and Technologies m) Unified Endpoint Management; Page 56-57	Licensing metric	Confirm licensing model: per device, per user, bundled with E3/E5, or other	Licensing shall be per device.
85	4.4 Deployment of Security Tools and Technologies m) Unified Endpoint Management; Page 56-57	Security controls	Scope for patch management, encryption (BitLocker/FileVault), remote wipe, DLP, and USB/device control	Tender Conditions Prevail. No Change
86	4.4 Deployment of Security Tools and Technologies m) Unified Endpoint Management; Page 56-57	HA / DR requirement	Clarify high availability and disaster recovery requirements for UEM infrastructure	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:44:48 +05'30'

87	4.4 Deployment of Security Tools and Technologies m) Unified Endpoint Management; Page 56-57	SIEM integration	Specify SIEM platform and expected alert forwarding / correlation requirements	Tender Conditions Prevail. No Change
88	4.4 Deployment of Security Tools and Technologies m) Unified Endpoint Management; Page 56-57	Project timeline	Expected project duration, phase-wise rollout vs full rollout, and pilot environment requirements	Please refer Clause 8 of page no. 17 for outline of works be carried in the Tender document
89	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	PAM	How many number of privileged users are you looking for a PAM solution to be implemented	All users across the organisation
90	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	PAM	How many numbers of assets needs to be on boarded onto PAM	All endpoint users as covered in EDR clause no. 31 in page no.109 of the Tender Document

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:45:08 +05'30'

91	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	PAM	What are the kind of assets that needs to be integrated to the PAM.	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
92	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	PAM	What kind of deployment is BESCOM looking for PAM. For e.g., Standalone, DC-DR, HA in DC-DR etc.	Please refer the note mentioned below in this document
93	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	PAM	What kind of thick client based/exe-based applications used by customer that needs to be on boarded onto PAM. Kindly help with the names of these applications if any.	For Application list please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:45:27 +05'30'

94	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	PAM	What kind of a deployment is the customer looking for ? For instance, on premises/cloud/hybrid.	On premises
95	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	SSO and MFA	Please share the indicative list of applications and users to be integrated with SSO (cloud, on prem, custom), along with their authentication capabilities (SAML/OIDC only, form based, etc.)	For Application list please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document
96	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	SSO and MFA	Please clarify whether SSO is required for internal users only, or also for external users (partners, customers, vendors) and whether CIAM/B2B/B2C use cases are in scope.	This is to clarify that SSO is required for internal users & also for external users

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:45:47 +05'30'

97	4.4 Deployment of Security Tools and Technologies n) Identity and Access Management (IAM) Integration; Page 57	SSO and MFA	Please specify the mandatory MFA methods (e.g., TOTP app, push notification, FIDO2/WebAuthn security keys, hardware tokens, SMS/email OTP as backup only).	This is to clarify that MFA methods can be TOTP, push notification
98	5.16. Post-Contract Emergency Support: The tenderer shall provide emergency support even beyond the contract period (Five years after Go-Live) until BESCOM transitions to a new service provider or in house operations.		Duration not clear. Please clarify.	Please refer Clause 5.16 in page no.66 of the tender document. Tender Condition prevail

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:46:11 +05'30'

99	Section 5 – Objectives (2.1)	"SIEM and SOAR platforms shall be deployed in separate and dedicated instances for IT and OT environments to ensure strict segregation, independent monitoring, and controlled incident response across enterprise IT and operational technology networks."	Kindly confirm whether separate hardware infrastructure is required for IT and OT instances or logical segregation within the same infrastructure is acceptable	Tender Conditions Prevail. No Change
100	Section 5 – Objectives (2.2)	Real time monitoring of all logs with log aggregation having SIEM & SOAR to collect & monitor logs effectively.	Kindly confirm the expected log retention duration and storage requirements under the scope of SIEM.	Please refer Clause 17 in page no.84 of the tender document
101	Section 5 – 4.6 (Functional Requirement of Tools and Technologies)	Live data feeds from SIEM and other integrated systems with refresh interval ≤ 30 seconds.	Kindly clarify whether the ≤30 seconds refresh interval applies to all dashboards including executive dashboards or only operational SOC dashboards	This is to clarify that ≤30 seconds refresh interval applies to all dashboards
102	Section 5 – 4.7 (General Requirements)	The selected tenderer should perform integration of CSOC with existing BESCOM IT/OT/IoT network, mobile, web applications, applications/services hosted in public cloud and security solutions of BESCOM. The selected tenderer is also responsible for any future integrations post final acceptance at no additional cost to BESCOM."	Kindly clarify whether integrations with third-party tools introduced after Go-Live but outside the current scope shall be considered under Change Request mechanism	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:46:34 +05'30'

103	Section 5 – SLA Note	At any point in time, if the solution is not able to handle the committed EPS count, the solution will be considered as DOWN and corresponding SLAs shall be applicable.”	Kindly clarify the methodology for measuring committed EPS count and whether any burst tolerance is permissible.	Tender Conditions Prevail. No Change
104	Section 5 – EDR Requirement	For the remaining years of the CSOC project/contract period or after expiry of the existing EDR contract, the C-SOC tenderer shall provide EDR deployment (if required), licensing, and full SIEM/SOAR integration.”	Kindly confirm whether EDR deployment scope includes servers, workstations, and other endpoints across IT and OT environments	Yes
105	Section 5 – EDR Requirement	BESCOM reserves the right to increase or decrease the number of endpoints during the contract period.	Kindly clarify the commercial adjustment mechanism in case of increase in endpoint count during the contract period.	Please refer Clause no.31 in Page no. 109 of the tender document. Tender conditions prevail.
106	5.Multi Factor Authentication & Single Sign On, Page number 150	The OEM must have cloud hosting available in India as the organisation may like to partly or fully transition from on-prem to partly or fully cloud environment in the future.	Please confirm whether the cloud hosting requirement may be fulfilled through either an OEM-managed SaaS deployment or infrastructure hosted in India regions of approved hyperscalers such as AWS, Microsoft Azure, or Google Cloud.	This is to clarify that MFA shall be hosted on-premises as of now and shall be moved to cloud (Infrastructure hosted in India) when required.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:46:56 +05'30'

107	5.Multi Factor Authentication & Single Sign On, Page number 150	The OEM must demonstrate strong innovation capability by providing examples, eg: having atleast 1 internationally recognized patent or innovative features developed.	Please confirm whether innovative IAM features or product recognitions can be considered equivalent to patent criteria.	Tender Conditions Prevail. No Change
108	5.Multi Factor Authentication & Single Sign On, Page number 150	There must be an SME deployed by the OEM to ensure successful implementations. If necessary, the OEM must be ready to provide a permanent team member to implementation & managed services teams.	Kindly clarify whether this is mandatory onsite deployment or remote engagement is acceptable.	Onsite deployment
109	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must allow the organization to expand the solution to other IAM modules without additional installation.	Please confirm whether enabling additional modules via license activation (without reinstallation) meets the requirement.	Yes
110	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must provide a centralized identity platform (Universal Identity directory) to view, manage & administer all types of user identities in the organization.	Kindly confirm whether integration with existing AD as primary identity store with virtual directory capability is acceptable.	Please refer Specification No.5. Multi Factor Authentication & Single Sign in Page no.151 of the tender document.
111	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must integrate with existing on-premises directory services such as Active Directory (AD) or LDAP.	Please confirm if bidirectional synchronization is required or read-only integration is sufficient.	Yes, bidirectional synchronization is required

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:47:17 +05'30'

112	5.Multi Factor Authentication & Single Sign On, Page number 151	The solutions must have the out-of-the-box connector built for various SoT systems and applications.	Kindly share the list of specific SoT systems (HRMS/ERP) currently in scope.	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
113	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must include SSO for thick-client and thin clients-on MS Windows.	Kindly clarify whether Windows Integrated Authentication (WIA/Kerberos) support will suffice.	It is acceptable, provided it doesn't require separate authentication and integrates with SSO
114	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must restrict any direct access to non-federated web applications.	Please clarify whether reverse proxy / secure access gateway approach is expected.	Reverse proxy or secure access gateway approach is acceptable for restricting direct access to non-federated web applications, provided the solution delivers full visibility, access control, and audit logging for all application access attempts.
115	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must support Password less Authentication. (Leverage native device authentication factors or Out-of-band Authentication with a Mobile Application) The solution must support password less Authentication as an MFA for Core Banking Applications.	Kindly clarify the specific authentication mechanisms that will be considered compliant with the "passwordless authentication" requirement under this clause.	Push notification via OEM mobile authenticator app is required. TOTP is acceptable. SMS OTP is permissible as backup only, not as primary authentication.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:47:38 +05'30'

116	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must support out-of-the-box authentication factors such as Email OTP, SMS OTP, Soft-token etc.	Please confirm whether SMS gateway will be provided by BESCOM or expected to be arranged by bidder.	By the bidder
117	5.Multi Factor Authentication & Single Sign On, Page number 151	Audit, Compliance, and Reporting	Kindly confirm expected log retention period and archival policy.	Please refer Section 5. Detailed Scope of Work, Clause 17 in page no. 84 of the tender documents.
118	5.Multi Factor Authentication & Single Sign On, Page number 151	The solution must integrate with SIEM tool	Please confirm the SIEM product currently used and expected integration mechanism (Syslog/API).	SSO/IAM solution shall integrate with any proposed NG-SIEM via Syslog/CEF for complete audit log forwarding (authentication events, access violations, privilege escalations) and REST API for correlated incident management. and should support SIEM connector's
119	5.Multi Factor Authentication & Single Sign On, Page number 151	General	Kindly confirm the total number of users and the expected peak concurrent users to be considered for sizing and architecture of the proposed IDAM solution.	Nearly 6000~ end points
120	5.Multi Factor Authentication & Single Sign On, Page number 151	General	Kindly confirm the total number and classification of applications (web, legacy, thick client, etc.) to be integrated with the IDAM solution, along with the phase-wise rollout plan.	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:47:59 +05'30'

121	5.Multi Factor Authentication & Single Sign On, Page number 151	General	Kindly confirm whether High Availability (HA) is required in both Primary (DC) and Disaster Recovery (DR) environments, and whether the DR setup is expected to be a full replica of the DC environment.	Yes
122	5.Multi Factor Authentication & Single Sign On, Page number 151	General	Kindly provide the expected implementation schedule from the date of award, including phase-wise timelines and milestone deliverables.	Please refer Clause 8 in page no.17of the tender document
123	5.Multi Factor Authentication & Single Sign On, Page number 150	The OEM must demonstrate strong innovation capability by providing examples, eg: having atleast 1 internationally recognized patent or innovative features developed	As we are doing implementation in India, Please let us know the need for international experience, Please elaborate on this point.	Tender Conditions Prevail. No Change
124	Page no.127 clause no.7	SIEM solution must apply intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions using Agentic AI and GEN AI	GEN AI and Agentic AI for faster triaging will require cloud connection. While all other SIEM features are available for air gapped environment as well.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:48:25 +05'30'

125	Page no.131 clause no.61	The data storage and indexing component should provide the ability to scale "horizontally", meaning the capability to start with a set of nodes within a single data store/cluster and keep adding additional nodes to handle larger volumes of data without having the need to replace or upgrade the existing nodes in the cluster. Alternate Clause: The data storage and indexing component should provide the ability to scale "horizontally and vertically", meaning the capability to start with a set of nodes within a single data store/cluster and keep adding additional nodes to handle larger volumes of data without having the need to replace or upgrade the existing nodes in the cluster.		Tender Conditions Prevail. No Change
126	Page no.135	SOAR and TIP requirement	Request if SOAR and TIP requirements can be separate section instead of a merged section as both solutions are different	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:48:51 +05'30'

127	Page no.136 clause no.26	Solution should track all forensic data related to an incident in one location (s system images, snapshots etc) and view the history of evidence across the entire incident	System image and snapshot are not SOAR capabilities, request if these can be moved to relevant section	Tender Conditions Prevail. No Change
128	Page no.138 clause no.81	Solution should have an option to configure and manage the SOC shifts within the	SOAR manages users, roles, and permissions effectively. However, a dedicated "Shift Roaster" module to manage personnel clock-in/clock-out or rotations is not a native core feature. Request if this can be removed.	Tender Conditions Prevail. No Change
129	Page no.164 clause no.3	The proposed solution must support full packet capture/ smart Capture.	Alternate clause suggested: The proposed solution must support full packet capture/ smart Capture/Flow based. Justification: As the asked feature also include flow based solution.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:49:14 +05'30'

130	Page no.165 NBAD-NDR : 14	Network Detection and Response (NDR) solutions leverage the inherent packet/ flow technologies present in network devices. These tools should possess the capability to capture packets from ongoing streams of real-time network traffic and transform this raw data into actionable analytics represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes.	Alternate clause suggested: Network Detection and Response (NDR) solutions leverage the inherent packet/ flow technologies present in network devices. These tools should possess the capability to provide visibility to real-time network traffic and transform this raw data into actionable analytics represented through numerical data, charts, and tables. This analytical output serves to quantify precisely how the network is utilized, by whom, and for what purposes. Justification : As asked product feature include flow technology which doesn't work on packet capture, hence requesting change without diluting the ask functional ask	Tender Conditions Prevail. No Change
131	Page no.166 NBAD-NDR : 44	The solution should have DNS Threat Analytics Capability to detect the threat present in DNS traffic.	Alternate clause suggested: Please remove the clause as the functionality is not related NDR and can be delivered through SIEM/SOAR	Tender Conditions Prevail. No Change
132	Page no.166 NBAD-NDR : 45	The solution should have capability to detect DNS tunnelling.	Alternate clause suggested: Please remove the clause as the functionality is not related NDR and can be delivered through SIEM/SOAR	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:49:36 +05'30'

133	Page no.167 NBAD-NDR : 48	The solution should be able to analyse SMTP traffic to detect high volume email, abnormal patterns in email traffic, traffic from unfriendly countries and with character sets often used by attackers (ex. Chinese).	Alternate clause suggested: The solution should be able to analyse SMTP traffic to detect high volume email, abnormal patterns in email traffic. Justification: For content and character based control you require email gateway solution. This is not a NBAD functionality	Tender Conditions Prevail. No Change
134	Page no.168 NBAD-NDR : 73	The system should have a mechanism to consume external lists of known bad IP's and generate alerts on the same if connection is seen.	Alternate clause suggested: Please remove the clause. can be delivered through SIEM/SOAR	Tender Conditions Prevail. No Change
135	Page no.168 NBAD-NDR : 74	The NDR system should be able to integrate with external threat feeds.	Alternate clause suggested: Please remove the clause. can be delivered through SIEM/SOAR	Tender Conditions Prevail. No Change
136	Page no.168 NBAD-NDR : 76	The solution should have native integration with CERT CMTX & NCIIPC Threat Feeds.	Alternate clause suggested: Please remove the clause. can be delivered through SIEM/SOAR	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:49:58 +05'30'

137	Page no.168 NBAD-NDR : 87	NDR device should be capable to support 10Gbps traffic throughput from day one without any hardware upgradation and should have 4 x 1/10G (copper) traffic capture/ monitoring ports and 2 x 1G management ports along with 5Gbps license from day one. Full packet capture needs to be planned with 7 days retention of PCAP files.	Alternate clause suggested: NDR device should be capable to support 10Gbps traffic throughput or 10,000 flows per second from day one without any hardware upgradation and should have 4 x 1/10G (copper) traffic capture/ monitoring ports and 2 x 1G management ports along with 5Gbps license from day one. Justification: Request to include sizing as per flows per second also as some OEM's license based on flows. Request you to delete the full packet capture clause.	Tender Conditions Prevail. No Change
138			Advisory/Supplementary Clause: The proposed SIEM, SOAR and UEBA must be from the same OEM.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:50:21 +05'30'

139			Advisory/Supplementary Clause: The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	Tender Conditions Prevail. No Change
140			Advisory/Supplementary Clause: Machine learning should be embedded across the platform (SIEM, SBDL & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:51:07 +05'30'

141			Advisory/Supplementary Clause: The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO.	Tender Conditions Prevail. No Change
142			Advisory/Supplementary Clause: The proposed solution must support a configurable replication factor of N where it can tolerate the failure of N-1 peer nodes or should handle failure of a node in the solution.	Tender Conditions Prevail. No Change
143		Despite multiple attempts, this tender is not visible, searchable, or available on the KPPP portal, making it impossible for us to access documents or submit our bid before the deadline.	This is a time-sensitive matter as the submission deadline is approaching shortly. We request your urgent assistance to: Confirm whether the tender is active and accessible on the portal Share the direct link to the tender page Clarify if there are any access restrictions or technical issues Consider extending the submission deadline if the visibility issue persists, as it may affect fair participation	BANGALORE ELECTRICITY SUPPLY COMPANY LIMITED Tender Reference: BESCOM/2025-26/SE0441 Portal https://kppp.karnataka.gov.in

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:51:59 +05'30'

144	30. Exit Management; Page no.107	In the event of termination or expiry of the Contract, both the Contractor and BESCOM shall comply with the provision of Exit plan. During the exit management period, the Contractor uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, products, software licenses, tools, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.	Kindly requesting to amend the clause as "In the event of termination or expiry of the Contract, both the Contractor and BESCOM shall comply with the provision of Exit plan. During the exit management period, the Contractor uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, software licenses, tools, reports, documents, manuals, data and web content to BESCOM.	Tender Conditions Prevail. No Change
145	Technical Specification 2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP); Page no.137	63. Solution should support open standard formats like CyboX, OpenIOC, Yara, STIX 1.0, STIX 2.0, MISP, XML, CSV, JSON, MAEC, IODEF etc.	kindly amend the clause as " Solution should support open standard formats like CyboX/OpenIOC, Yara/STIX 1.0, STIX 2.0, MISP, XML, CSV, JSON/MAEC/IODEF etc."	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:52:26 +05'30'

146	Technical 2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP); Page no.137	64. Solution should also be capable of supporting unstructured formats such as email, news, RSS Feeds, blogs, Free text etc. and should be capable of automatically normalizing it.	kindly amend the clause as " Solution should also be capable of supporting unstructured formats such as email/news, RSS Feeds, blogs/ Free text etc. and should be capable of automatically normalizing it."	Tender Conditions Prevail. No Change
147	Cyber Security Operation Centre Bill of Quantities 17 Training & Knowledge Transfer; Page 218		Kindly specify the number of personnel and the duration of the training	Tender Conditions Prevail. No Change
148	B C-SOC Room Infra; Page no.219	Log Collectors in HA (in active-passive mode of operation) - Pair 4 The quantity considered per Discom includes Log Collector per network i.e. OT, DR, Enterprise IT applications , IT Public facing.	a) According to the RFP, the deployment of solutions is in DC, so we understand that a separate OPLC is mandatorily required in DC. Please confirm on this. If yes, the OPLC count will be 5 pair. b) Please confirm whether log data needs to be collected from any remote locations in addition to this.	a) Yes b) Yes

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:52:58 +05'30'

149	Pre-bid meeting		The Pre-Bid Meeting will be held offline. Please provide an online option for the pre-bid meeting. We would like to address our concerns related to the tender.	Pre Bid meeting was held on 19.02.2026.
150	Pre-bid meeting		Upon further reviewing the entire tender document and after discussing with prospective bidders, we kindly request you to provide us time till 26th February to submit the pre-bid queries and clarifications. As our bidders/SI's have to review the entire, kindly allow us additional time.	Tender Conditions Prevail. No Change
151	Page 138	The WAF and Anti-DDoS services shall be integrated to ensure seamless security with high efficiency and shall be from same OEM. Further, no separate traffic redirection shall be configured by BESCOM for WAF and Anti-DDoS services.	For traffic redirection DNS diversion needs to be done.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:53:24 +05'30'

152	Page 139	No hardware & software is to be installed at Origin Web server/DC for the provisioning of the Cloud WAF security services. However, for Internal Applications that are not exposed publicly, The proposed solution should also support an out-of-path API-based cloud application security architecture to optimally protect internal applications deployed in Datacentre which cannot be DNS routable over the internet (using same WAAP service plan) . This service should integrate on-premise load balancing or reverse proxy solution (includingRadware, F5, Ngnix, HA Proxy etc). via plugin/connector.	Do we need to factor internal applications for BoM?	Yes.
153	Page 140	Should provide Service Level Commitment of minimum 99.999% at least with Service Credits	Please elaborate on service credit	Please refer SLA Table-1 in page no.116 of the tender document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:53:53 +05'30'

154			Please provide sizing inputs from licensing perspective - 1. API parameters 2. BoT protection parameters 3. WAF parameters 4. DDoS parameters (bandwidth coverage, Hybrid/Always On)	The sizing of all proposed technology solutions shall be determined by the bidder based on the Bill of Quantities (BOQ) provided in the tender document and the Events Per Second (EPS) specifications mentioned therein. The bidder shall ensure that the proposed infrastructure, licences, and platform capacities are adequately sized to meet the EPS thresholds & scope defined in the BOQ for the entire duration of the contract, including provisions for peak load and future growth. Any under-sizing or performance degradation attributable to incorrect sizing by the bidder shall be the sole responsibility of the bidder and shall not constitute grounds for additional cost claims against BESCOM.
155	Page 56	Implement a hybrid (cloud + on-premises) DDoS mitigation solution.	Pg 50 of tender document says DDoS solution is Cloud + On-Premises, however on-prenises clause is not there in the compliance section. Please clarify.	Tender conditions prevail as mentioned Section 5. Detailed Scope of Work.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:54:20 +05'30'

156		General	In order to calculate the hardware sizing and license count, please provide following details NMS 1. No of network devices to be monitored along with the bifurcation (routers, switches, firewalls, servers, UPS and any other SNMP devices) Helpdesk 1. No of technicians for Helpdesk	Please refer Scope of Coverage Section in page no. 125 of Tender Document.
157	Monitoring entire network, links, systems, devices, applications, etc. for availability, performance, SLA and other parameters using tools. Page 59	Monitoring entire network, links, systems, devices, applications, etc. for availability, performance, SLA and other parameters using tools.	Do BESCOM require NMS as well? If yes please define functional and technical requirement along with No of devices to be monitored	Tender conditions prevail.-No change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:54:47 +05'30'

158	Page 150 In the technical specification stated that - "The proposed solution should be a "Make in India Class 1" Product."	Kindly clarify the criteria for qualification under “Make in India Class 1 Product.” Specifically, please confirm whether the presence of an OEM development center in India, along with substantial value addition within India, would be considered compliant with this requirement.	The term “Make in India Class 1 Product” is governed by specific DPIIT guidelines relating to local content percentage. Clarification is required to understand the evaluation criteria and documentation expectations. This will ensure accurate compliance confirmation and submission of appropriate supporting documents during technical evaluation.	Tender Conditions Prevail. No Change
159	Page 150 The solution should have a single source code. It shouldn't be different modules integrated into one single dashboard.	The solution should be from same OEM & It should be tightly integrated in dashboard.	Alert: Strictly Vendor specific clause. It restricts participation. Clause to be modifed / deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change
160	Page 170 Clause No.11,11.5 Allow easy translation of findings into monitoring rules	To be classisfied as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:55:14 +05'30'

161	Page 170 Clause No.11,11.6 Configuration lock-down & change tracking of the policies on the solution	To be classified as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change
162	Page 170 Clause No.11,11.9 Proposed solution should support 6000+ VA tests e.g. weak passwords, missing patches, CSI benchmark, PCI-DSS regulations, vulnerable codes etc.	To be classified as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:55:41 +05'30'

163	Page 170 Clause No.11,11.8 Does the product provide actionable reports (e.g. recommended SQL conmmands to solve issues discovered by the tool)	To be classisfied as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change
164	Page 55 clause 4.4 Deployment of Security Tools and Technologies	Deploy EDR agents across all enterprise endpoints, servers, and critical OT systems.	Request to confirm the total number of critical OT endpoint system	Approx. 250 nos. of critical OT endpoint system
165	Page 55 clause 7 End point Detection & Response	The proposed solution should provide on-premises virtual server component which will be hosted at the customer data centre in a forward proxy mode for any communication between endpoints and the OEM's EDR solution.	Kindly confirm whether OT network is having connection with the forward proxy to comply connection with OEM's EDR solution as per RFP request.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:56:13 +05'30'

166	Page 220; Annual Maintenance Cost	SIEM and SOAR Integration Only – Existing EDR Endpoints (1303): Integration of existing EDR server with SIEM/SOAR, security event correlation, alerting, and incident analysis. No EDR deployment or licensing applicable.	Please confirm when will the existing EDR contract end ?	Please refer Clause 31 in page 109 of the tender document
167	Page 220; Annual Maintenance Cost	SIEM and SOAR Integration Only – Existing EDR Endpoints (1303): Integration of existing EDR server with SIEM/SOAR, security event correlation, alerting, and incident analysis. No EDR deployment or licensing applicable.	Please confirm whether these 1303 endpoints are incluided the 6000 EDR as requirement ?	Please refer Clause 31 in page no. 109 of the tender document
168	Page 218; Table 2 : Cyber Security Operation Centre Bill of Quantities	Service Edge(SSE)/Proxy Gateway	Please share the sizing details and specification for the SSE solution	Shall be sized based on the number of users as mentioned in page no.125 of Tender Document
169	Page 165; Clause 10; NBAD-NDR	The solution should have the capability of application profiling in the system and also support custom applications present or acquired by the end user.	Request to change statement as "The solution should have the capability to identify and control network traffic based on protocol and application characteristics, with support for creating custom detection rules and filters to address specific applications present or acquired by the end user"	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:56:49 +05'30'

170	Page 165; Clause 10; NBAD-NDR	The solution should have the capability to enrich flow records with additional fields including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, number of packets and number of bytes transmitted in a session, timestamps for start and end of session, NAT translations, etc. from captured data and then utilize those fields in analytical algorithms to alarm on anomalous behaviours.	Request to change the statement as "The solution should have the capability to capture and analyze network traffic metadata including source and destination IPs, MAC addresses, TCP/UDP ports or ICMP types and codes, packet and byte counts, session timestamps, and other relevant protocol fields from inspected traffic. The solution should utilize this information in analytical algorithms to detect and alarm on malicious activities and security anomalies."	Tender Conditions Prevail. No Change
171	Page 165; Clause 10; NBAD-NDR	The solution must be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.	Request to change the statement as "The solution must be able to track security-relevant host and user activities at monitored network segments and should be able to report on threat detections, affected systems, and security events across the deployed infrastructure. When integrated with a centralized management platform, the solution should provide correlated visibility across multiple deployment sites"	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:57:20 +05'30'

172	Page 165; Clause 10; NBAD-NDR	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL or packet capture based solution.	Request to change the statement as "The solution should provide network visibility through flow-based monitoring (including support for industry-standard flow protocols such as sFlow) and/or deep packet inspection capabilities. The solution may support integration with external flow collectors or packet broker infrastructure to accommodate additional flow protocol requirements."	Tender Conditions Prevail. No Change
173	Page 165; Clause 10; NBAD-NDR	The solution should be able to analyze SMTP traffic to detect high volume email, abnormal patterns in email traffic, traffic from unfriendly countries and with character sets often used by attackers (ex. Chinese).	Request to change the statement as "The solution should be able to inspect SMTP protocol traffic to detect malicious email-borne threats, suspicious attachments, phishing attempts, command-and-control communications, and traffic patterns associated with known threat actors. The solution should leverage threat intelligence including geographic reputation data and threat indicators to identify and block email-based attacks."	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:57:53 +05'30'

174	Page 165; Clause 10; NBAD-NDR	The solution should support active scanning of specific enterprise assets in addition to passive profiling of devices on the network	Request to change the statement as "The solution should support passive detection and profiling of devices, protocols, and threats through inline or mirrored network traffic inspection. The solution should provide continuous visibility into network assets and security events based on observed traffic patterns and threat intelligence."	Tender Conditions Prevail. No Change
175	Page 165; Clause 10; NBAD-NDR	Solution should come with predefined & customisable reports and should have ability to run certain reports based on security role.	Request to change the statement as "The solution should provide security dashboards and reporting capabilities with pre-built views for threat trends, security events, and system health metrics. The management interface should support customizable dashboard widgets and report components. The solution should implement role-based access controls allowing administrators to assign different visibility and reporting permissions based on user roles and responsibilities."	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:58:27 +05'30'

176	Page 165; Clause 10; NBAD-NDR	The solution should have an automated scanner to identify assets and should also be able to schedule the scan	Request to change the statement as "The solution should provide automated asset visibility and threat detection through continuous passive network traffic monitoring. The solution should maintain awareness of active hosts, network devices, and communication patterns observed within monitored network segments"	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:59:00 +05'30'

177	Section 5, 20. Threat Modelling & Use Case Requirements: Clause 20.6	The entire SIEM/SOC solution including log storage, analytics, dashboards, and SOAR must be hosted and processed fully On-Premise.	The RFP mandates "in-built AI & ML capabilities" True AI/ML requires massive compute power available only in the cloud to analyze behavioral patterns across global datasets. On-premise hardware is limited in its ability to detect sophisticated zero-day attacks in real-time. SaaS platforms eliminate the risk of hardware obsolescence and scale instantly to handle the 25,000 EPS requirement without requiring BESCOM to procure additional hardware later. Will BESCOM allow a Cloud-Native / SaaS-based Unified Security Operations Platform (SIEM + SOAR + TIP + ASM+ EDR/XDR) hosted within a MeitY-empaneled Data Center in India? Please clarify.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 15:59:36 +05'30'

178	1. Security Incident and Event Management (SIEM)> Sl. No. 61	The data storage and indexing component should provide the ability to scale "horizontally", meaning the capability to start with a set of nodes within a single data store/cluster and keep adding additional nodes to handle larger volumes of data without having the need to replace or upgrade the existing nodes in the cluster.	Specifying "adding nodes" ties the solution to hardware management. A SaaS platform eliminates the burden of infrastructure sizing and node management, offering instant elasticity for peak loads without hardware procurement delays. Will BESCOM accept a SaaS-based delivery model where the backend scaling (compute/storage) is managed transparently by the OEM, guaranteeing performance SLAs (25K EPS) without need to manually "add nodes" or manage clustering?	Tender Conditions Prevail. No Change
179	1. Security Incident and Event Management (SIEM)> Sl. No. 85	Solution should be able to provide raw and normalized logs/data storage as per the retention requirements for SIEM technology as outlined in the scope of work in this RFP	Mandating "fully On-Premise" processing prevents the use of hyperscale AI/ML models required for advanced threat detection. Hosting data in an India-based cloud ensures Data Residency compliance (DPDP Act) while unlocking superior security analytics. Will BESCOM allow the "Processing and Storage" plane to be hosted in a MeitY-Empaneled Cloud Data Center within India while keeping the Log Collectors on-premise?Please clarify.	Please refer note mentioned below in this document

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:00:13 +05'30'

180	1. Security Incident and Event Management (SIEM)> Sl. No. 89	Raw, normalized correlated logs shall be stored to the attached storage/SAN/NAS for the future reference and forensic activities in the event of incident.	The RFP mandates "in-built AI & ML capabilities". Cloud-scale compute is required to run advanced ML models for threat detection effectively, which is not feasible with on-premise hardware limitations. Using a hybrid model ensures BESCOM retains full sovereignty over the data (On-Premise storage) for forensic/legal needs, while utilizing the cloud solely for detection logic. Will BESCOM allow a Hybrid Architecture where the heavy security analytics (AI/ML processing) are performed in a MeitY-empaneled Cloud (SaaS), while the Raw Logs and Long-Term Storage are retained On-Premise via a log forwarder/broker? Please clarify.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:00:58 +05'30'

181	2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP)> Sl. No. 1	Solution should be able to deploy on-prem virtual machine or cloud-based with the same license.	SaaS-based SOAR platforms provide faster time-to-value, instant integration with cloud apps and receive immediate AI/ML updates for playbooks. This technical specification explicitly allows "Cloud-based" deployment, which contradicts Section 5, Clause 20.6 mandating "fully On-Premise" hosting. Please amend Clause 20.6 to align with this Technical Spec (Sl. No. 1), thereby allowing a SaaS-delivered SOAR & TIP hosted in a MeitY-empaneled Data Center.	Tender Conditions Prevail. No Change
182	2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP)> Sl. No. 68	Solution must provide additional information on IOCs, wherever requested, by integrating with WHOIS, Virus total, Shodan, Hybrid Analysis etc.	These services require paid enterprise API keys for high-volume automated lookups. Clarification is needed to ensure all bidders include these significant costs. Please confirm if the Commercial Subscriptions/API Keys for these 3rd party services (VirusTotal, Shodan, etc.) are to be provided by BESCOM, or if the 1Bidder must factor these subscription costs into the commercial bid?	All the subscription charges to be borne by the successful bidder.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:01:47 +05'30'

183	7. End point Detection & Response>SI .No. 6	The proposed solution should have but not limited to the following prevention capabilities: Antimalware with signature/Pattern based detection Ransomware protection Machine learning - pre-execution and runtime Browser exploit protection Behavior monitoring Injection protection Script protection Anti-exploit C&C communication prevention Application control File less malware prevention File/web reputation	We request to change the specification as below: The proposed solution should have but not limited to the following prevention capabilities: Antimalware with signature/Pattern based detection Ransomware protection Machine learning - pre-execution and runtime Browser exploit protection Behavior monitoring Injection protection Script protection Anti-exploit C&C communication prevention File less malware prevention	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:02:32 +05'30'

184	7. End point Detection & Response>SI .No. 14	The solution must have an integrated Application Control module to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities(llow or prevent users from changing settings or unloading/uninstalling the software).	We request to remove this speciifcation	Tender Conditions Prevail; No Change
185	7. End point Detection & Response>SI .No. 21	Shall be able to scan Object Linking and Embedding (OLE) File.	This is OEM specific clause, We request to remove this specification	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:03:07 +05'30'

186	7. End point Detection & Response>SI .No. 29	The solution must support legacy and rare operating systems including but not limited to the below mentioned operating system: a. Microsoft Windows 10,11, Windows Server 2012 & 2012 R2, 2016,2019, 2022 b. RHEL 6,7,8 ,9 c. CentOS 6,7,8 d. Ubuntu 16,18,20 & 22 e. Debian 8,9,10 & 11 f. Solaris 10.0,11.0,11.1,11.2,11.3,11.4 g. Oracle Linux 6,7,8,9 h. AIX 6.1,7.1,7.2 & 7.3 i. SUSE Linux 12,15 j. MacOS BigSur, Monterey, Ventura, Sonoma, Sequoia	We request to remove the EOL declared OS from the specification. The solution must support legacy and rare operating systems including but not limited to the below mentioned operating system: a. Microsoft Windows 10,11, Windows Server 2012 & 2012 R2, 2016,2019, 2022 b. RHEL 6,7,8 ,9 c. CentOS 6,7,8 d. Ubuntu 16,18,20 & 22 e. Debian 9,10 & 11 f. Oracle Linux 6,7,8,9 g. SUSE Linux 12,15 h. MacOS Monterey, Ventura, Sonoma, Sequoia	Tender Conditions Prevail. No Change
187	7. End point Detection & Response>SI .No. 37	Must have a host-based intrusion prevention system (HIPS) to virtually patch known and unknown vulnerabilities before a patch is available or deployable.	We request to remove this speciifcation	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:03:43 +05'30'

188	In the technical specification stated that - "The proposed solution should be a "Make in India Class 1" Product."	The solution should be from same OEM & It should be tightly integrated in dashboard.	The term “Make in India Class 1 Product” is governed by specific DPIIT guidelines relating to local content percentage. Clarification is required to understand the evaluation criteria and documentation expectations. This will ensure accurate compliance confirmation and submission of appropriate supporting documents during technical evaluation.	Tender Conditions Prevail. No Change
189	The solution should have a single source code. It shouldn't be different modules integrated into one single dashboard.		Alert: Strictly Vendor specific clause. It restricts participation. Clause to be modifed / deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change
190	Allow easy translation of findings into monitoring rules	To be classisfied as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:04:22 +05'30'

191	Configuration lock-down & change tracking of the policies on the solution	To be classisfied as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change
192	Proposed solution should support 6000+ VA tests e.g. weak passwords, missing patches, CSI benchmark, PCI-DSS regulations, vulnerable codes etc.	To be classisfied as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change
193	Does the product provide actionable reports (e.g. recommended SQL conmmands to solve issues discovered by the tool)	To be classisfied as optional as this is not a feature of DAM tool	Alert: Feature dependent on only specific & strictly to VA Tool. Vendor specific clause. It restricts participation. Clause to be deleted for level playing opportunity for all OEMs / Vendors / MSIs.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:04:55 +05'30'

194	Page 127 clause 7	SIEM solution must apply intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions using Agentic AI and GEN AI	Kindly amend the clause to allow intelligent analytics and threat intelligence–driven investigation within the SIEM, with AI/ML capabilities provided through integrated solutions	Tender Conditions Prevail. No Change
195	Page 129 clause 29	Solution must be capable of providing real time and on demand access to data sources such as evolving format, Custom API's, interfaced incl. text, XML, JSON, Data Base connections, Network Ports, Connections or from log data., and files	ArcSight SIEM supports real-time and on-demand access to security data by ingesting information from diverse sources using SmartConnectors, FlexConnectors, and APIs supporting formats such as text, XML, and JSON, and supports databases, files, logs, and network ports (e.g., Syslog).	Tender Conditions Prevail. No Change
196	Page 130 clause 45	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability for security alert in Window Unix and Linux environment. to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment.	The project is for Security operations. Clause to be amended as mentioned in column F or have it deleted (Delete it since Infrastructure monitoring is not part of a security operations)	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:05:32 +05'30'

197	Page 131 clause 64	The solution should have the capability to add as many fields/columns in the index. The solution should support any number of fields in a particular row of data and should be able to store any amount of data in a particular field	Kindly amend the clause since - Number of Field, columns and field data size should be defined to a permissible limit and cannot be infinite.	Tender Conditions Prevail. No Change
198	Page 136 clause 20	Solution should be capable of implementing a new integration without any coding requirment and should support no code based implementation.	Kindly amend the clause to mention 'low-code' as custom intgegrations will require low/code supprt.	Tender Conditions Prevail. No Change
199	Page 136 clause 26	Solution should track all forensic data related to an incident in one location (s system images, snapshots etc) and view the history of evidence across the entire incident	Kindly amend the clause as mentioned on Column F OR clarify if forensic related artifacts need to the uploaded to the ticketing component within the solution	Tender Conditions Prevail. No Change
200	Page 137 clause 57	Solution should be able to identify coverage gaps by identifying missing mandatory controls in the environment.	Kindly elaborate on the use case requirement.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:09:42 +05'30'

201	Page 138 clause 81	Solution should have an option to configure and manage the SOC shifts within the platform	Kindly clarify that SOC shift management refers to role- and schedule-based assignment of incidents and tasks rather than full workforce rostering.	Tender Conditions Prevail. No Change
202	SIEM; Suggested Clause	SIEM solution should be licensed based on standard licensing parameter (i. e. sustained events per second) and should be perpetual. Licenses should be considered for non-production sites (DR, UAT, DEV, TESTING) to benefit customer without any surplus license cost during the tenure of the project.	As per industry standard	Tender Conditions Prevail. No Change
203	SIEM; Suggested Clause	SIEM and Prevention Security solutions like F/W, Packet Capture, IPS, HIPS, AV, DLP, NDR, EDR, NBAD, Router, Switches etc should be from different OEM. So that it can detect threats missed by other existing tools using the security defence in depth strategy.	As per industry standard	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:10:05 +05'30'

204	SIEM; Suggested Clause	Quoted SIEM Solution must have its presence in India for more than 15 years and must have at least 3 deployments for more than 30000 EPS in Government of India organization. At least 3 sign-off must be attached for more than 30K EPS from Government of India organization. Customer Signoff need to be provided at the time of bidding.	As per industry standard	Tender Conditions Prevail. No Change
205	SIEM; Suggested Clause	SOAR capabilities within SIEM must not require any separate license and with no restriction on number of analysts. In case SOAR is not native or from different OEM, License should be proposed for 18 analysts.	As per industry standard	Tender Conditions Prevail. No Change
206		As per the RFP, we see the inclusion of ITSM and ITAM in the scope of work, however this is not included part of the BOQ	Kindly request you to include part of the BOQ and give us a clarity on the same.	Everything mentioned in the tender document has to be scoped in the project.
207	SECTION 7: Payment Terms and Milestones – C-SOC Implementation	As per the RFP, it is stated that "Payment for Human Resources will be paid on a monthly basis after the implementation phase, and payment for subscription will be paid annually."	We request clarification on whether the annual subscription payment will be made in advance at the start of each subscription period and similarly for the Human Resources	Payments will not be made in advance in any case.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:10:30 +05'30'

208	Generic Query	No. of Mobile Apps & Volumetrics	Kindly confirm on the number of mobile application(s) to be included, along with the annual active user count for each application and the projected user volumes over the contract tenure.	Please refer Scope of Coverage Section in page no. 124 of Tender Document.
209	SECTION 7: Payment Terms and Milestones – C-SOC Implementation Page no 217	II. Payment for Human Resources: Will be paid on monthly basis after the implementation phase. III. Payment for subscription: Will be paid annually.	As per the RFP, it is stated that "Payment for Human Resources will be paid on a monthly basis after the implementation phase, and payment for subscription will be paid annually." We request clarification on whether the annual subscription payment will be made in advance at the start of each subscription period and similarly for the Human Resources	Payments will not be made in advance in any case.
210	Generic Query	No. of Mobile Apps & Volumetrics	Kindly confirm on the number of mobile application(s) to be included, along with the annual active user count for each application and the projected user volumes over the contract tenure.	Please refer Scope of Coverage Section in page no. 124 of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:10:56 +05'30'

211	External Attack Surface Management 15 Point No 6	Phishing, Pharming, Brand Abuse, rouge websites and mobile apps related to BESCOM, Email address used for fraudulent purpose.	Phishing, Brand Abuse, rouge websites and mobile apps related to BESCOM, Email address used for fraudulent purpose. We request to remove Pharming as it is OEM specific	Tender Conditions Prevail; No Change
212	External Attack Surface Management Page no 15 Point No 6	Solution should provide a security configuration index score that summarizes deployed and missing security controls within the environment.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
213	External Attack Surface Management Page no161 Point No 14	Incorporate asset criticality, vulnerabilities, threat activity and configuration of security controls in the calculation of risk score for each asset type.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
214	External Attack Surface Management Page no 162 Point No 15	Should be able to list all domains and respective subdomains belonging to the organization and provide domain discovery trend data monthly for at least one year.	We request to amend the point as - Should be able to list all domains and respective subdomains belonging to the organization	Tender Conditions Prevail. No Change
215	External Attack Surface Management Page no 162 Point No 16	Should be able to list all Public IP addresses belonging to the organization and provide IP asset discovery trend data monthly over time for at least one year.	We request to amend the point as - Should be able to list all Public IP addresses belonging to the organization	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:11:34 +05'30'

216	External Attack Surface Management Page no 162 Point No 19	Should be able to show an asset graph for each domain and IP asset. An asset graph graphically illustrates the asset's connection to internal assets in the environment.	We request to amend the point as - Should be able to show an asset graph for each domain and IP asset.	Tender Conditions Prevail. No Change
217	External Attack Surface Management Page no 162 Point No 20	Provide an asset criticality score per domain and IP asset. Asset criticality indicates	We request to amend the point as - Provide an asset criticality score per domain and IP asset. Asset criticality indicates the importance of an asset in an organization.	Tender Conditions Prevail. No Change
218	External Attack Surface Management Page no 162 Point No 26	Should be able to show an asset graph for each device asset. An asset graph graphically illustrates the asset's connection to other assets in the environment.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
219	External Attack Surface Management Page no 162 Point No 27	Provide an asset criticality score per device asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:12:02 +05'30'

220	External Attack Surface Management Page no 162 Point No 29	Should be able to list all discovered internal device assets and show discovery trend monthly over time for at least one year.	Yes, we request to amend the point as - Should be able to list all discovered internal device assets	Tender Conditions Prevail. No Change
221	External Attack Surface Management Page no 162 Point No 30	Show device asset's cloud application usage and activity	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
222	External Attack Surface Management Page no 162 Point No 33	Show device assets logged on users including username, email address, location, job title and user risk score.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
223	External Attack Surface Management Page no 162 Point No 34	Provide an asset criticality score per device asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:12:31 +05'30'

224	External Attack Surface Management Page no 162 Point No 35	Provide a summary of a device asset by building an asset profile. Details should include basic device info (OS, device type, group membership, etc), Activity, Device Usage, Connection information, Influence, and Identity posture risk.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
225	External Attack Surface Management Page no 162 Point No 39	Should be able to provide the account's latest risk score, user type, role, location, job title and when the account was first and last seen	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
226	External Attack Surface Management Page no 162 Point No 42	Provide an account criticality score for both domain and service account. Account criticality indicates the importance of the account in an organization. Administrators should be able to manually change the account criticality rating.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
227	External Attack Surface Management Page no 162 Point No 44	Enumerate application roles granted to discovered service accounts.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:12:58 +05'30'

228	External Attack Surface Management Page no 162 Point No 45	Enumerate granted consent permissions to discovered service accounts.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
229	External Attack Surface Management Page no 162 Point No 46	Should be able to list all discovered accounts and show account discovery trend monthly over time for at least one year.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
230	External Attack Surface Management Page no 162 Point No 47	Show account's cloud application usage and activity.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
231	External Attack Surface Management Page no 162 Point No 49	Show account's activity by displaying logon data location on map.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
232	External Attack Surface Management Page no 162 Point No 50	Show account's latest account risk score, user type, role, location, job title and when the account was first and last seen.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:13:31 +05'30'

233	External Attack Surface Management Page no 162 Point No 51	Provide a summary of an account by building an asset profile. Details should include basic account info (level, role, group membership, etc), Activity, Device Usage, Email usage information, Influence, and Identity posture risk.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
234	External Attack Surface Management Page no 162 Point No 53	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Highly Exploitable unique CVEs.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
235	External Attack Surface Management Page no 162 Point No 54	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Mean Time to Patch	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
236	External Attack Surface Management Page no 162 Point No 55	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Average Unpatched Time	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:13:57 +05'30'

237	4.4 Deployment of Security Tools and Technologies: Page no 55	Deploy EDR agents across all enterprise endpoints, servers, and critical OT systems.	Request to confirm the total number of critical OT endpoint system	Tender Conditions Prevail. No Change
238	7. End point Detection & Response Page no 55	The proposed solution should provide on-premises virtual server component which will be hosted at the customer data centre in a forward proxy mode for any communication between endpoints and the OEM's EDR solution.	Kindly confirm whether OT network is having connection with the forward proxy to comply connection with OEM's EDR solution as per RFP request.	Tender Conditions Prevail. No Change
239	Annual Maintenance Cost Page no 220	SIEM and SOAR Integration Only – Existing EDR Endpoints (1303): Integration of existing EDR server with SIEM/SOAR, security event correlation, alerting, and incident analysis. No EDR deployment or licensing applicable.	Please confirm when will the existing EDR contract end? Please confirm whether these 1303 endpoints are included the 6000 EDR as requirement ?	Tender Conditions Prevail. No Change
240	Table 2 : Cyber Security Operation Centre Bill of Quantities Page no 218	Service Edge(SSE)/Proxy Gateway	Please share the sizing details and specification for the SSE solution	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:14:23 +05'30'

241	10. NBAD-NDR Page no 165	The solution should have the capability of application profiling in the system and also support custom applications present or acquired by the end user.	Request to change statement as "The solution should have the capability to identify and control network traffic based on protocol and application characteristics, with support for creating custom detection rules and filters to address specific applications present or acquired by the end user"	Tender Conditions Prevail. No Change
242	10. NBAD-NDR Page no 165	The solution should have the capability to enrich flow records with additional fields including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, number of packets and number of bytes transmitted in a session, timestamps for start and end of session, NAT translations, etc. from captured data and then utilize those fields in analytical algorithms to alarm on anomalous behaviors	Request to change the statement as "The solution should have the capability to capture and analyze network traffic metadata including source and destination IPs, MAC addresses, TCP/UDP ports or ICMP types and codes, packet and byte counts, session timestamps, and other relevant protocol fields from inspected traffic. The solution should utilize this information in analytical algorithms to detect and alarm on malicious activities and security anomalies."	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:14:52 +05'30'

243	10. NBAD-NDR Page no 165	The solution must be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.	Request to change the statement as "The solution must be able to track security-relevant host and user activities at monitored network segments and should be able to report on threat detections, affected systems, and security events across the deployed infrastructure. When integrated with a centralized management platform, the solution should provide correlated visibility across multiple deployment sites"	Tender Conditions Prevail. No Change
244	10. NBAD-NDR Page no 165	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL or packet capture based solution.	Request to change the statement as "The solution should provide network visibility through flow-based monitoring (including support for industry-standard flow protocols such as sFlow) and/or deep packet inspection capabilities. The solution may support integration with external flow collectors or packet broker infrastructure to accommodate additional flow protocol requirements."	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:15:18 +05'30'

245	10. NBAD-NDR Page no 167	The solution should be able to analyze SMTP traffic to detect high volume email, abnormal patterns in email traffic, traffic from unfriendly countries and with character sets often used by attackers (ex. Chinese)	Request to change the statement as "The solution should be able to inspect SMTP protocol traffic to detect malicious email-borne threats, suspicious attachments, phishing attempts, command-and-control communications, and traffic patterns associated with known threat actors. The solution should leverage threat intelligence including geographic reputation data and threat indicators to identify and block email-based attacks."	Tender Conditions Prevail. No Change
246	10. NBAD-NDR Page no 167	The solution should support active scanning of specific enterprise assets in addition to passive profiling of devices on the network	Request to change the statement as "The solution should support passive detection and profiling of devices, protocols, and threats through inline or mirrored network traffic inspection. The solution should provide continuous visibility into network assets and security events based on observed traffic patterns and threat intelligence."	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:15:45 +05'30'

247	10. NBAD-NDR Page no 168	Solution should come with predefined & customisable reports and should have ability to run certain reports based on security role.	Request to change the statement as "The solution should provide security dashboards and reporting capabilities with pre-built views for threat trends, security events, and system health metrics. The management interface should support customizable dashboard widgets and report components. The solution should implement role-based access controls allowing administrators to assign different visibility and reporting permissions based on user roles and responsibilities."	Tender Conditions Prevail. No Change
248	10. NBAD-NDR Page no 168	The solution should have an automated scanner to identify assets and should also be able to schedule the scan	Request to change the statement as "The solution should provide automated asset visibility and threat detection through continuous passive network traffic monitoring. The solution should maintain awareness of active hosts, network devices, and communication patterns observed within monitored network segments"	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:16:15 +05'30'

249	site survey Page no 62		Do we need to upload any site survey report or cetificate	Yes
250	MAF/ OEM Letter		MAF required from OEM	Yes
251	Page no 134	Proposed SIEM solution should have capabilities to be integrate with SOAR, EMS/NMS, ITSM etc.	integrate with Existing EMS/NMS.ITSM or Do we need to quote, there is no specification for this.	The SIEM must be capable of integrating with existing or future systems added as part of C-SOC such as SOAR, EMS/NMS, ITSM, etc.
252	4.7 General requirement SOC Rom Setup Page no 62	All the tools supplied as part of the project should be supplied with Enterprise grade Licenses	SOC Rom Setup required for server room and infra setup(desk) in DC. The DR required only Server room setup and not required work desk and interior, DC and DR Connectivity and preferred location.	Please refer note mentioned below in this document

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:16:45 +05'30'

253	Virtualization Page no 60	All the tools supplied as part of the project should be supplied with Enterprise grade Licenses	Proxmox with Premium support consider like Enterprise grade Licenses	Tender Conditions Prevail. No Change
254	30. Exit Management Page no 107	In the event of termination or expiry of the Contract, both the Contractor and BESCOM shall comply with the provision of Exit plan. During the exit management period, the Contractor uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, products, software licenses, tools, source codes, reports, documents, manuals, data, web content and other intellectual property rights to BESCOM.	Kindly requesting to amend the clause as "In the event of termination or expiry of the Contract, both the Contractor and BESCOM shall comply with the provision of Exit plan. During the exit management period, the Contractor uses its best efforts to continue delivery of all regular services. In addition, the successful tenderer shall ensure that complete handover of the processes, software licenses, tools, reports, documents, manuals, data and web content to BESCOM.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:17:15 +05'30'

255	2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP) Page no 137	63. Solution should support open standard formats like CyboX, OpenIOC, Yara, STIX 1.0, STIX 2.0, MISP, XML, CSV, JSON, MAEC, IODEF etc.	kindly amend the clause as " Solution should support open standard formats like CyboX/OpenIOC, Yara/STIX 1.0, STIX 2.0, MISP, XML, CSV, JSON/MAEC/IODEF etc."	Tender Conditions Prevail. No Change
256	2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP) Page no 137	64. Solution should also be capable of supporting unstructured formats such as email, news, RSS Feeds, blogs, Free text etc. and should be capable of automatically normalizing it.	kindly amend the clause as " Solution should also be capable of supporting unstructured formats such as email/news, RSS Feeds, blogs/ Free text etc. and should be capable of automatically normalizing it."	Tender Conditions Prevail. No Change
257	Cyber Security Operation Centre Bill of Quantities 17 Training & Knowledge Transfer Page no 218		Kindly specify the number of personnel and the duration of the training	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:17:46 +05'30'

258	B C-SOC Room Infra Page no 219	Log Collectors in HA (in active-passive mode of operation) - Pair 4 The quantity considered per Discom includes Log Collector per network i.e. OT, DR, Enterprise IT applications , IT Public facing.	a) According to the RFP, the deployment of solutions is in DC, so we understand that a separate OPLC is mandatorily required in DC. Please confirm on this. If yes, the OPLC count will be 5 pair. b) Please confirm whether log data needs to be collected from any remote locations in addition to this.	a.) Yes b.) Yes

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:18:17 +05'30'

259	Page 216 SECTION 7 Payment Terms and Milestones – C-SOC Implementation	I. Payment for One Time Setup Cost: RFP defines the payment milestones for one time setup cost as 55 percent on supply 25 percent on installation and commissioning and 20 percent after FAT UAT and 6 months successful operation	Considering the significant upfront procurement and implementation cost involved in establishing the solution infrastructure we request the authority to kindly revise the payment terms to 80 10 10 to ensure smoother project execution and cash flow alignment Proposed payment terms 80 percent on supply delivery inspection and acceptance of BoM items 10 percent on successful installation commissioning and readiness certification 10 percent on successful FAT UAT and submission of required reports We request the authority to kindly consider and amend the clause accordingly	Tender condition prevails as tool integration is very important.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:18:49 +05'30'

260	Page 212, 213 SCC Clause SC2 Liquidated Damages Page 212 Pages 116 122 SLA penalties	Overall penalty 10 percentage	We understand that the RFP includes penalty provisions for service level non compliance Considering the long term nature and operational dependency of the project multiple factors including external integrations third party dependencies and customer infrastructure may impact service levels despite best efforts To ensure balanced contractual risk and wider participation we request the authority to kindly cap the overall cumulative penalty under the contract to a maximum of 5 percent of the contract value We request the authority to amend the clause accordingly	Tender Conditions Prevail. No Change
261	SECTION 5: DETAILED SCOPE OF WORK 2. Objectives of the Project Page NO.49	SIEM and SOAR platforms shall be deployed in separate and dedicated instances for IT and OT environments to ensure strict segregation, independent monitoring, and controlled incident response across enterprise IT and operational technology networks.	Kindly clarify whether separate and dedicated SIEM and SOAR instances are mandatory for IT and OT environments, and please confirm whether separate hardware infrastructure is required for IT and OT deployments. Please confirm the same deployment of SIEM & SOAR should be done on DR as well.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:30:14 +05'30'

262	SECTION 5: DETAILED SCOPE OF WORK 2. Objectives of the Project Page NO.50	Governance, risk management, and compliance (GRC) by aligning with ISO/IEC 27001:2022, NIST CSF, CERT-In advisories and CEA Cyber Security Guidelines 2021 or latest	Kindly confirm whether deployment of a dedicated GRC tool is require for this project. If yes than it should be install primary in DC and replica in DR.	Yes, dedicated GRC tools needs to be deployed.
263	h) Network and Connectivity Page No. 52	Network and Security Appliances: The server room shall accommodate and support the deployment of following components(to be supplied, configured, and maintained by the tenderer as per BoQ): Next-Generation Firewalls (NGFW) with UTM features, Intrusion Detection and Prevention Systems (IDPS), Layer 2 / Layer 3 Switches, Network Load Balancers, VPN Gateways and other edge security devices	1.Kindly provide detailed technical specifications and performance requirements for NGFW, IDPS, VPN gateways to enable accurate sizing. 2. Please explain the meaning of other edge security devices 3.Kindly confirm the expected number of concurrent remote VPN users Also confirm the NGFW should be install in DR also	Shall be sized based on the number of users as mentioned in Scope of Coverage Section in page no. 125 of Tender Document..
264	4.4 Deployment of Security Tools and Technologies: d) Endpoint Detection & Response (EDR) Page No.55	Endpoint Detection & Response (EDR)	Kindly confirm the total number of endpoints (desktops, laptops, servers, and virtual machines) to be covered under the EDR solution, along with OS bifurcation and also confirm the EDR should be install in DR also.	Total Number of EDR is 6000~. Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:30:54 +05'30'

265	4.4 Deployment of Security Tools and Technologies: Implement a comprehensive vulnerability scanning solution covering IT, OT, IoT, and cloud systems.	Implement a comprehensive vulnerability scanning solution covering IT, OT, IoT, and cloud systems.	Kindly confirm the total number of IT, OT, IoT, and cloud assets to be covered under the Vulnerability Management solution, along with scan frequency, credentialed scan requirements. And Also confirm the deployment of VA should be in Dc and DR also.	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
266	4.4 Deployment of Security Tools and Technologies: h) Mobile Application Security (RASP	Integrate Runtime Application Self-Protection (RASP) for BESCOM's mobile applications. · Enable detection of runtime threats, including tampering, reverse engineering, malicious code injection, and API misuse	Kindly confirm the number of mobile applications (Android/iOS), estimated monthly active users, and whether source code access will be provided for RASP integration. Please confirm the RASP should be install in DR also.	Please refer scope of coverage clause in page No. 124 & 125 of Tender Document for number of mobile applications. Yes, RASP should be in DR also.
267	4.4 Deployment of Security Tools and Technologies: i) Infrastructure and Cloud On boarding	On-board BESCOM's on-premises and cloud infrastructure (private and public) into the SOC monitoring framework. Configure connectors, APIs, and telemetry to achieve unified monitoring, alerting, and compliance visibility.	Kindly confirm the detailed inventory of on-premises, private cloud, and public cloud assets to be on boarded into SOC, including total log sources, estimated log volume (EPS/GB per day), retention requirements, and integration scope, to enable accurate SIEM sizing.	Private cloud/Public cloud details shall be provided to the successful bidder. For estimated log volume please ref-SIEM Specification Sl no. 08 in Page No.128 of the tender document. For retention details please refer Clause no.16 in Page No 83 of the tender document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:31:24 +05'30'

268	4.4 Deployment of Security Tools and Technologies: j) External Attack Surface Management (EASM)	Identify and monitor BESCOM's external-facing assets, including domains, IPs, and web services. · Detect shadow IT, misconfigurations, certificate expirations, and exposed data. · Integrate findings with SIEM for continuous risk assessment.	Kindly confirm the total number of domains, subdomains, public IP ranges, cloud environments, and externally exposed assets to be monitored under EASM, along with expected scan frequency and SIEM integration requirements, to enable accurate sizing estimation.	Since Domain, Sub domain, IP ranges are confidential those details cannot be shared. For sizing please ref Scope coverage section in Page No 124 & 125 of the tender document.
269	4.4 Deployment of Security Tools and Technologies: k) DDoS Protection	· Implement a hybrid (cloud + on-premises) DDoS mitigation solution. · Configure detection and scrubbing mechanisms for volumetric, protocol, and application-layer attacks.	Kindly confirm whether a dedicated on-premises DDoS mitigation appliance is require as part of the hybrid solution, or if cloud-based DDoS protection integrated with existing perimeter devices will be acceptable. Also please confirm on the total internet bandwidth, peak traffic capacity, number of public IPs. Please confirm whether the DDOS appliance should require in HA in DC and DR as well	Since proposed CSOC is on-premises solution, DDOS mitigation appliances is required in HA in DC &DR as well.
270	4.4 Deployment of Security Tools and Technologies l) Web Application Firewall (WAF) and API Security	Deploy WAF to safeguard web portals, APIs, and mobile backends.	Kindly confirm the number of web applications, APIs, and mobile backends, expected traffic throughput (Mbps/Gbps), SSL termination requirements and HA configuration in DC and DR requirement	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:32:01 +05'30'

271	4.4 Deployment of Security Tools and Technologies: m) Unified Endpoint Management (UEM)	· Onboard enterprise desktops, laptops, and mobile devices into the UEM solution.	Kindly confirm the total number of desktops, laptops, and mobile devices (with OS bifurcation), whether BYOD devices are in scope, and patching coverage requirements (OS and third-party applications), and HA (DC/DR) requirements,	All together projected as 6000~ endpoints. Please refer clause 31 in page No.109 of the tender document.
272	4.4 Deployment of Security Tools and Technologies: n) Identity and Access Management (IAM) Integration	· Integrate Single Sign-On (SSO) with enterprise AD/LDAP or Identity Provider. · Implement Multi-Factor Authentication (MFA) and role based access for all administrative accounts.	Kindly confirm the total number of users and administrative accounts, number of applications to be integrated with SSO, existing AD/LDAP/IdP environment details, MFA mechanism, and HA (DC/DR) requirements,	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document for number of Application to be integrated to SSO.
273	4.4 Deployment of Security Tools and Technologies: n) Identity and Access Management (IAM) Integration	Deploy Privileged Access Management (PAM) to monitor and control administrator activity.	Please confirm whether PAM need to deploy. If yes than provide the total number of privileged accounts, target systems (servers, network devices, databases, cloud), session recording requirements, and DC/DR deployment expectations.	Please refer section n) Identity and Access Management (IAM) Integration in Page No 57 of the tender document, to be deployed in DC & DR.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:32:33 +05'30'

274	4.4 Deployment of Security Tools and Technologies: o) Ticketing Tool – ITSM and ITAM	o) Ticketing Tool – ITSM and ITAM	Kindly confirm the total asset volume across IT, cloud, virtualized, and OT environments, expected CMDB discovery scope, number of custom workflows to be configured, SLA/OLA complexity for NGSOC, reporting requirements, and governance integration expectations, Please also cofirm the ITSM should be deploy in DC & DR	Tender Conditions Prevail. No Change
275	4.5 Outline of Tasks to be Carried Out Under Implementation of C SOC:	Provide total anti-phishing, brand monitoring services for BESCOM and BESCOM 's internet facing IT/OT/IoT web and mobile applications.	Kindly confirm whether brand monitoring including phishing domain detection, is expected as part of the EASM solution or as a separate Digital Risk Protection service.	Tender Conditions Prevail. No Change
276	4.5 Outline of Tasks to be Carried Out Under Implementation of C SOC:	Provide forensics/incident response support as per the requirement of BESCOM in case of any incident	Kindly clarify the expected scope of forensic and incident response support, including response SLA, number of incidents covered annually, onsite vs remote requirement, severity classification, and whether forensic investigations are included within base scope or to be charged on a per-incident basis,	Forensic & incident response support to be provided through out the contract period as part of scope coverage detailed in Tender document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:33:07 +05'30'

277	4.7 General Requirements:	Conducting regular DC-DR drills for the proposed solutions.	Kindly confirm whether all proposed solutions deployed at the Primary Data Center (DC) are required to be implemented at the Disaster Recovery (DR) site as well, Also confirm on High availablity for proposed solution in DR	Yes, DC-DR drills are required
278	5. Human Resource Details: 5.8.1. SOC Team: 65	L3 SOC Specialist – 01 No (onsite dedicated resource 24×7×365 availability for escalations and critical support)	Kindly clarify whether the L3 resource is required to be available in a 24×7 shift rotation, or if the L3 resource can work in general business hours with on-call support for escalations during non-business hours.	L3 Resourse shall work in General shift as per table mentioned in clause no 5.18 & shall be available in person 24x7x365 in case of emergency situation.
279	5. Human Resource Details: 5.17. General requirement of all resources: Page No.67	The SOC Manager shall ensure that adequate human resource is available to meet the deliverables as per the scope of work and maintain performance and availability requirements as per SLA.	Kindly clarify whether the SOC Manager is required to be deployed as a full-time dedicated resource for this engagement.	L3 analyst shall perform the duty of SOC manager as well.
280	11. Business Continuity and Disaster Recovery Plan Page No. 78	11.14. Forensic Data Preservation: Collect and preserve all relevant logs, memory images, and evidence in a tamper-proof manner to support root cause analysis, regulatory reporting, and possible legal proceedings.	Kindly confirm whether forensic evidence storage infrastructure will be provided by BESCOM	Forensic evidence storage infra to be part of proposed CSOC setup infra.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:33:43 +05'30'

281	11. Business Continuity and Disaster Recovery Plan Page No. 78	11.19. Crisis Management & Tabletop Exercises: Periodically conduct tabletop simulations and mock drills (Red Team / Blue Team exercises) to test and validate BESCOM's readiness to handle large scale incidents.	Kindly clarify how often Crisis Management and Table top Exercises (including Red Team / Blue Team simulations) are required, the scope and coverage of these activities, stakeholder involvement, and reporting requirements. Additionally, please confirm whether these activities are to be treated as separate services	These are part of scope of work as mentioned in clause 11.19. crisis management & table top exercises in page 78 of the tender document to be conducted as and when requested by BESCOM Scope & stakeholder involvement details shall be provided during execution. These activities are not to be treated as separate services.
282	12. Threat Intelligence and Proactive Defense Page No. 79	TTP Analysis & Adversary Profiling: Analyze threat actor behavior, campaigns, and infrastructure to build Threat Models and anticipate potential attack vectors against BESCOM.	Kindly clarify the expected frequency, depth, and deliverables of TTP analysis and adversary profiling, including reporting format, sector-specific intelligence requirements,	As detailed in technical Specification of SOAR & TIP. Please refer clause 12. Threat Intelligence and Proactive Defence in Page No. 79 of Tender document.
283	13. SECURITY INCIDENT ANALYSIS AND FORENSICS Page No. 80	Malware & Payload Analysis: Analyze malicious files, binaries, or scripts using sandboxing and reverse-engineering techniques to understand capabilities, persistence mechanisms, and potential lateral movement.	Kindly clarify whether BESCOM currently has any existing tools for sandboxing and reverse engineering, or if the bidder is expected to provide and implement these tools as part of the project scope.	Yes, the bidder is expected to provide and implement these tools as part of the project scope.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:34:17 +05'30'

284	18.4. Solution Integration, Commissioning, and Go-Live Page No.88	Simulated Attack Drills: The tenderer shall conduct controlled red team/blue-team exercises and mock cyberattack simulations to validate SOC detection and response readiness before go-live.	Kindly confirm wehther the BESCOM will provide the tools for red team/blue-team exercises and mock cyberattack simulations or tenderer will provide the same.	Bidder shall provide the necessary tools for red/blue team as detailed in tender clause.
285	23. Training Page No.90	Tabletop and Hands-on Exercises: The tenderer shall conduct periodic incident simulation drills (phishing, ransomware, insider threat, DDoS, OT compromise) to build response maturity and improve Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).	Kindly clarify the frequency, scope, and technical depth of the Tabletop and Hands-on incident simulation drills (phishing, ransomware, insider threat, DDoS, OT compromise), expected reporting and MTTD/MTTR measurement methodology, and confirm whether the required simulation tools will be provided by BESCOM or need to be procured by the tenderer,	Frequency of table top and hands-on exercises shall be as per CERT-In guidelines and as and when requested by BESCOM. Simulation tools / techniques shall be provided by the successful bidder.
286	SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP) Page 135	Solution should be able to deploy on-prem virtual machine or cloud-based with the same license.	Kindly clarify whether the requirement is for a standalone Threat Intelligence Platform (TIP) for centralized feed management and operationalization, or if integrated threat intelligence services within SOAR/SIEM solutions are acceptable.	There shall be a standalone TIP for centralized feed management and operationalization and the same has to be integrated with the CSOC services.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:34:52 +05'30'

287	SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP) Page 135	Solution should be able to deploy on-prem virtual machine or cloud-based with the same license.	Kindly clarify whether cloud deployment of the SOAR and Threat Intelligence Platform is permitted, as the RFP also mandates that the entire SIEM/SOC solution must be fully hosted On-Premise. Additionally, please confirm whether the requirement of “same license for On-Prem and Cloud deployment” is applicable under the current scope or intended for future scalability.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:35:24 +05'30'

288	5. Multi Factor Authentication & Single Sign On II Converged IAM Platform Page No. 150	The SSO solution must have capabilities to extend to converged IAM capabilities, including Access Management (AM), Identity Governance and Administration (IGA), and Privileged Identity & Access Management (PIAM), with all IAM modules (AM, IGA, PIAM) present in a single code base, providing a unified administration interface for IGA, PIAM, and Access Management functionalities, managing all IDAM use cases and tasks from a single dashboard or interface, and offering a comprehensive IAM framework encompassing IGA, PIAM, and AM functionalities.	Kindly clarify whether the requirement of having Access Management (AM), Identity Governance & Administration (IGA), and Privileged Identity & Access Management (PIAM) in a single code base is mandatory, or whether an integrated IAM suite from the same OEM with unified administration interface and seamless interoperability between modules will be acceptable.	Tender Conditions Prevail. No Change
289	2. Payment Schedule Table 2 Cyber Security Operation Centre Bill of Quantities Page No. 218	Application Whitelisting & Secure Web Gateway (SWG)/Secure	Kindly clarify this requirement, as no specific technical details have been provided in the RFP.	Please refer Scope of Coverage Section in page no. 125 of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:36:00 +05'30'

290	2. Payment Schedule Table 2 Cyber Security Operation Centre Bill of Quantities Page No. 218	Service Edge(SSE)/Proxy Gateway	Kindly clarify this requirement, as no specific technical details have been provided in the RFP.	Shall be sized based on the number of users as mentioned in Scope of Coverage Section in page no. 125 of Tender Document
291	2. Payment Schedule Table 2 Cyber Security Operation Centre Bill of Quantities Page No. 218	Air-Gapped IT/OT Secured Communication (IT/OT Appliance)	Kindly clarify this requirement, as no specific technical details have been provided in the RFP.	There shall be a logical Air gap gateway with Hardware data Diode.
292	External Attack Surface Management page no 15 Point No 6	Phishing, Pharming, Brand Abuse, rouge websites and mobile apps related to BESCOM, Email address used for fraudulent purpose.	We request to remove Pharming as it is OEM specific	Tender Conditions Prevail. No Change
293	External Attack Surface Management page no 161 Point No 13	Solution should provide a security configuration index score that summarizes deployed and missing security controls within the environment.	We request to remove Pharming as it is OEM specific	Tender Conditions Prevail. No Change
294	External Attack Surface Management page no 161 Point No 14	Incorporate asset criticality, vulnerabilities, threat activity and configuration of security controls in the calculation of risk score for each asset type.	We request to remove Pharming as it is OEM specific	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:36:35 +05'30'

295	External Attack Surface Management page no 161 Point No 15	Should be able to list all domains and respective subdomains belonging to the organization and provide domain discovery trend data monthly for at least one year.	We request to amend the point as - Should be able to list all domains and respective subdomains belonging to the organization	Tender Conditions Prevail. No Change
296	External Attack Surface Management page no 161 Point No 16	Should be able to list all Public IP addresses belonging to the organization and provide IP asset discovery trend data monthly over time for at least one year.	We request to amend the point as - Should be able to list all Public IP addresses belonging to the organization	Tender Conditions Prevail. No Change
297	External Attack Surface Management page no 161 Point No 19	Should be able to show an asset graph for each domain and IP asset. An asset graph graphically illustrates the asset's connection to internal assets in the environment.	We request to amend the point as - Should be able to show an asset graph for each domain and IP asset.	Tender Conditions Prevail. No Change
298	External Attack Surface Management page no 161 Point No 20	Provide an asset criticality score per domain and IP asset. Asset criticality indicates	We request to amend the point as - Provide an asset criticality score per domain and IP asset. Asset criticality indicates the importance of an asset in an organization.	Tender Conditions Prevail. No Change
299	External Attack Surface Management page no 161 Point No 26	Should be able to show an asset graph for each device asset. An asset graph graphically illustrates the asset's connection to other assets in the environment.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:37:12 +05'30'

300	External Attack Surface Management page no 161 Point No 27	Provide an asset criticality score per device asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
301	External Attack Surface Management page no 161 Point No 29	Should be able to list all discovered internal device assets and show discovery trend monthly over time for at least one year.	Yes, we request to amend the point as - Should be able to list all discovered internal device assets	Tender Conditions Prevail. No Change
302	External Attack Surface Management page no 161 Point No 30	Show device asset's cloud application usage and activity	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
303	External Attack Surface Management page no 161 Point No 33	Show device assets logged on users including username, email address, location, job title and user risk score.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
304	External Attack Surface Management page no 161 Point No 34	Provide an asset criticality score per device asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:37:49 +05'30'

305	External Attack Surface Management page no 161 Point No 35	Provide a summary of a device asset by building an asset profile. Details should include basic device info (OS, device type, group membership, etc), Activity, Device Usage, Connection information, Influence, and Identity posture risk.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
306	External Attack Surface Management page no 161 Point No 39	Should be able to provide the account's latest risk score, user type, role, location, job title and when the account was first and last seen	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
307	External Attack Surface Management page no 161 Point No 42	Provide an account criticality score for both domain and service account. Account criticality indicates the importance of the account in an organization. Administrators should be able to manually change the account criticality rating.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
308	External Attack Surface Management page no 161 Point No 44	Enumerate application roles granted to discovered service accounts.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:38:31 +05'30'

309	External Attack Surface Management page no 161 Point No 45	Enumerate granted consent permissions to discovered service accounts.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
310	External Attack Surface Management page no 161 Point No 46	Should be able to list all discovered accounts and show account discovery trend monthly over time for at least one year.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
311	External Attack Surface Management page no 161 Point No 47	Show account's cloud application usage and activity.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
312	External Attack Surface Management page no 161 Point No 49	Show account's activity by displaying logon data location on map.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
313	External Attack Surface Management page no 161 Point No 50	Show account's latest account risk score, user type, role, location, job title and when the account was first and last seen.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:39:14 +05'30'

314	External Attack Surface Management page no 161 Point No 51	Provide a summary of an account by building an asset profile. Details should include basic account info (level, role, group membership, etc), Activity, Device Usage, Email usage information, Influence, and Identity posture risk.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
315	External Attack Surface Management page no 161 Point No 53	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Highly Exploitable unique CVEs.	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
316	External Attack Surface Management page no 161 Point No 54	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Mean Time to Patch	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change
317	External Attack Surface Management page no 161 Point No 55	Provides vulnerability management metrics for both internal and Internet facing assets over time and be able to compare the organizations score to the global average. Metric: Average Unpatched Time	This is OEM specific Point. We request you to remove this.Point	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:39:51 +05'30'

318	Sl No 1 Page no 144	Integrated asset visibility, vulnerability detection, prioritization, remediation in one console	Remove vulnerability detection/scanning; keep device inventory only Vulnerability scanning is VM domain; not in UEM scope	Tender Conditions Prevail. No Change
319	Sl No 3 Page no 144	Detects vulnerabilities, misconfigurations, exposures	Remove vulnerability scanning; keep config compliance onlyVM responsibility, not UEM	Tender Conditions Prevail. No Change
320	Sl No 4 Page no 144	Patching: fixes all vulnerabilities, real-time analysis	Scope patching to Windows/macOS/Linux only; remove AIXMost UEMs do not support AIX patching	Tender Conditions Prevail. No Change
321	Sl No 7 Page no 144	Device discovery: automated scans, port/service/state detection	Remove network scans; restrict to enrolled devicesAgentless scanning is ITAM/Discovery, not UEM	Tender Conditions Prevail. No Change
322	Sl No 16 Page no 145	198 probes and 1470 attributes for discovery	Please Remove function of VM more than UEM, exact number is also vendor specific	Tender Conditions Prevail. No Change
323	Sl No 17 Page no 145	Air-gapped support	Make optional Cloud UEMs cannot operate air-gapped	Tender Conditions Prevail. No Change
324	Sl No 19 Page no 145	Agent-based/agentless scanning	Remove agentless scanning Not supported by top UEMs	Tender Conditions Prevail. No Change
325	Sl No 20 Page no 145	Multi-platform (30+ OS)	Limit to Windows/macOS/iOS/Android/ ChromeOSMost OEMs do not support 30+ OS	Tender Conditions Prevail. No Change
326	Sl No 21 Page no 145	License tracking, EOL/EOS detection	Make best-effort only Not uniform across OEMs	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:40:55 +05'30'

327	Risk Scoring Page no 145	Cyber hygiene scoring using vulnerabilities/misconfig	Remove vulnerability dependency Requires deep VM engine , not in UEM scope	Tender Conditions Prevail. No Change
328	Asset Exposure Page no 145	Continuous discovery incl. unmanaged/shadow IT	Move shadow IT discovery to ITAM Requires scanners not available in UEM tools	Tender Conditions Prevail. No Change
329	Vulnerability Management Page no 146	190k+ checks, 100% accuracy; agent/agentless; network/server/cloud scans	Remove VM section completely from UEM Belongs to VM scanners	Tender Conditions Prevail. No Change
330	Patch Management Page no 146	Windows/Linux/Mac/AIX/3rd party patching	Remove AIX and limit 3rd party catalog Most UEMs don't patch AIX or non supported OS by 3rd party	Tender Conditions Prevail. No Change
331	Endpoint Security Controls Page no 148	Isolation/quarantine, registry/kernel edits, remote shell	Remove or Move to EDR These are EDR functions	Tender Conditions Prevail. No Change
332	Reports Page no 149	1000s of APIs	Replace with "REST APIs" Numeric API counts are vendor-specific	Tender Conditions Prevail. No Change
333	Auditing Page no 150	Advanced user activity tracking	Need clarity on scope of tracking cannot track all activities of users , UEM cannot track activities performed within applications.	Tender Conditions Prevail. No Change
334	13 Page no 218	Unified Endpoint Management (UEM) | Lot | 1	Need breakup of licenses preferably by OS Needed for commercial evaluation - License for UEM and SSO are per user or per device based	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:41:42 +05'30'

335	C 3.5 Page no 220	UEM & SSO Licenses | Year | 5	Need breakup of licenses preferrably by by OSNeeded for commercial evaluation - License for UEM and SSO are per user or per device based	Please refer Section C. Tool AMC in Page no.221of Tender Document.
336	Sl. No. 2 Page no 138	WAF & Anti-DDoS integrated, same OEM; no separate traffic redirection by BESCOM.	Allow either same-OEM WAAP+DDoS or tightly integrated partner stack under a single MSP/OEM SLAMandating one OEM excludes strong pairs (e.g., WAAP+scrubbing combinations). A single-SLA operating model preserves accountability while broadening OEM participation.	Tender Conditions Prevail. No Change
337	Sl. No. 3 Page no 138	Cloud WAF, API Protection, BOT Mgmt, DDoS Mitigation from same Technology OEM.	Reword to “Cloud WAAP must include WAF, API security and Bot management from the OEM; DDoS may be same OEM or an OEM-grade integrated service under a unified SLA”This avoids excluding vendors with best-in-class WAAP plus integrated scrubbing clouds, while keeping a single pane-of-glass and SLA. There is already a separate DDoS solution required in the RFP	Tender Conditions Prevail. No Change
338	Sl. No. 4 Page no 138	≥50 PoPs globally, minimum 2 PoPs in INDIA.	Reword to " ≥2 in-country PoPs "A strict PoP count is vendor-specific	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:42:23 +05'30'

339	Sl. No. 5 Page no 138	Support Nokey feature for HSM integration; BESCOM keeps private key in HSM; no upload to cloud.	Make nokey/Keyless/HSM optionalOnly a few vendors offer nokey/keyless as part of their cloud offering	Tender Conditions Prevail. No Change
340	Sl. No. 6 Page no 138	No hardware/software at Origin/DC for Cloud WAF; support out-of-path API-based security for internal apps; integrate with on-prem load balancer via plugin/connector.	Request to removeCloud WAF is primarily for internet traffic, if security of internal apps (no internet edge) is required would suggest appliance to be installed on prem instead of Cloud WAF	Tender Conditions Prevail. No Change
341	Sl. No. 29 Page no 140	Web DDoS Protection add-on: behavioral detection, auto-signature, granular enforcement, L7 logic.	Would request the option to integrate with DDoS service with this functionality instead of being part of the WAF solution. Allows strong DDoS specialists while preserving operational simplicity and accountability. DDoS is already a separate solution as part of the RFP	Tender Conditions Prevail. No Change
342	Sl. No. 30–36 Page no 140	Bot Management features including crypto challenges, device attestation and mobile SDK.	Retain Bot Management as core; Replace remaining with " advanced Bot management" Different OEMs implement bot defenses differently (ML scoring vs. crypto puzzles). Optionalizing advanced methods widens competition.	Tender Conditions Prevail. No Change
343	Sl. No. 12 Page no 138	Protect apps regardless of origin (public/private cloud, on-prem); support HTTP/HTTPS.	Need clarity - that private Apps will have internet acces and DNS entryCWAF requires apps to have access to internet to function	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:43:06 +05'30'

344	Sl. No. 27 Page no 139	Provide managed certificates; automate generation/renewal; individual SSL per domain/sub-domain; no wildcard.	Allow wildcard certificates **or** SAN when policy permits; Allow option to use customer CA/PKI with HSM if requiredWill allow more OEMs as certificate management can be handled via separate service	Tender Conditions Prevail. No Change
345	A 12 Page no 218	WAF + API + Bot Protection	Kindly clarify breakup of applications, API and requests per minute to be secured under this service Needed for commercial evaluation	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
346	C 3.2 Page no 220	WAF / API / DDoS	Kindly clarify breakup of applications, API and requests per minute to be secured under this service Needed for commercial evaluation	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:43:46 +05'30'

347	Section 5, 20. Threat Modelling & Use Case 20.6 Requirements: Clause20.6 Page 89	The entire SIEM/SOC solution including log storage, analytics, dashboards, and SOAR must be hosted and processed fully On-Premise.	The RFP mandates "in-built Al & ML capabilities True AI/ML requires massive compute power available only in the cloud to analyze behavioral patterns across global datasets. On-premise hardware is limited in its ability to detect sophisticated zero-day attacks in real-time. SaaS platforms eliminate the risk of hardware obsolescence and scale instantly to handle the 25,000 EPS requirement without requiring BESCOM to procure additional hardware later. Will BESCOM allow a Cloud-Native/SaaS-based Unified Security Operations Platform (SIEM + SOAR + TIP + ASM+ EDR/XDR) hosted within a MeitY-empaneled Data Center in India? Please clarify.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:44:29 +05'30'

348	1. Security Incident and Event Management (SIEM)> Sl. No. 61 Page 131	The data storage and indexing component should provide the ability to scale "horizontally", meaning the capability to start with a set of nodes within a single data store/cluster and keep adding additional nodes to handle larger volumes of data without having the need to replace or upgrade the existing nodes in the cluster.	Specifying "adding nodes" ties the solution to hardware management. A Saas platform eliminates the burden of infrastructure sizing and node management, offering instant elasticity for peak loads without hardware procurement delays. Will BESCOM accept a SaaS-based delivery model where the backend scaling (compute/storage) is managed transparently by the OEM, guaranteeing performance SLAS (25K EPS) without need to manually "add nodes" or manage clustering?	Tender Conditions Prevail. No Change
349	1. Security Incident and Event Management (SIEM)> Sl. No. 85 Page 133	Solution should be able to provide raw and normalized logs/data storage as per the retention requirements for SIEM technology as outlined in the scope of work in this RFP	Mandating "fully On-Premise processing prevents the use of hyperscale Al/ML models required for advanced threat detection. Hosting data in an India-based cloud ensures Data Residency compliance (DPDP Act) while unlocking superior security analytics. Will BESCOM allow the "Processing and Storage" plane to be hosted in a MeitY-Empaneled Cloud Data Center within India while keeping the Log Collectors on-premise? Please clarify.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:45:12 +05'30'

350	1.Security Incident and Event Management (SIEM)> Sl. No. 89 page 134	Raw, normalized correlated logs shall be stored to the attached storage/SAN/NAS for the future reference and forensic activities in the event of incident.	The RFP mandates "in-built Al & ML capabilities. Cloud-scale compute is required to run advanced ML models for threat detection effectively, which is not feasible with on-premise hardware limitations. Using a hybrid model ensures BESCOM retains full sovereignty over the data (On-Premise storage) for forensic/legal needs, while utilizing the cloud solely for detection logic. Will BESCOM allow a Hybrid Architecture where the heavy security analytics (AI/ML processing) are performed in a MeitY-empaneled Cloud (SaaS), while the Raw Logs and Long-Term Storage are retained On-Premise via a log forwarder/broker? Please clarify.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:46:05 +05'30'

351	2. SOAR (Security Orchestration, Automated and Response) &Threat Intelligence Platform (TIP) Sl. No. 1 page 135	Solution should be able to deploy on-prem virtual machine or cloud-based with the same license.	SaaS-based SOAR platforms provide faster time-to-value, instant integration with cloud apps and receive immediate AI/ML updates for playbooks. This technical specification explicitly allows "Cloud-based deployment, which contradicts Section 5, Clause 20.6 mandating "fully On-Premise hosting. Please amend Clause 20.6 to align with this Technical Spec (51. No. 1), thereby allowing a Saas-delivered SOAR & TIP hosted in a Meity-empaneled Data Center.	Tender Conditions Prevail. No Change
352	2. SOAR (Security Orchestration.Automated and Response) &Threat Intelligence Platform (TIP)> Sl. No. 68 page 138	Solution must provide additional information on IOCs, wherever requested, by integrating with WHOIS, Virus total, Shodan, Hybrid Analysis etc.	These services require paid enterprise API keys for high-volume automated lookups. Clarification is needed to ensure all bidders include these significant costs. Please confirm if the Commercial Subscriptions/API Keys for these 3rd party services (VirusTotal, Shodan, etc.) are to be provided by BESCOM, or if the Bidder must factor these subscription costs into the commercial bid?	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:47:17 +05'30'

353	7. End point Detection & Response> S1.No. 6 page 152	The proposed solution should have but not limited to the following prevention capabilities: Antimalware with signature/Pattern based detection Ransomware protection Machine learning pre-execution and runtime Browser exploit protection Behavior monitoring Injection protection Script protection Anti-exploit C&C communication prevention Application control File less malware prevention File/web reputation	We request to change the specification as below: The proposed solution should have but not limited to the following prevention capabilities: Antimalware with signature/Pattern based detection Ransomware protection Machine learning pre-execution and runtime Browser exploit protection Behavior monitoring Injection protection Script protection Anti-exploit C&C communication prevention File less malware prevention	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:48:29 +05'30'

354	7. End point Detection & Response> Sl.No. 14 page 154	The solution must have an integrated Application Control module to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities(allow or prevent users from changing settings or unloading/uninstalling the software).	We request to remove this specification	Tender Conditions Prevail. No Change
355	7. End point Detection Et Response >Sl.No. 21 page 155	Shall be able to scan Object Linking and Embedding (OLE) File.	This is OEM specific clause, we request to remove this specification	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:49:07 +05'30'

356	End point Detection & Response >Sl.No. 29 Page 155	The solution must support legacy and rare operating systems including but not limited to the below mentioned operating system: a. Microsoft Windows 10,11, Windows Server 2012 & 2012 R2, 2016,2019, 2022 b. RHEL 6,7,8,9 c. CentOS 6,7,8 d. Ubuntu 16,18,20 & 22 e. Debian 8,9,10 & 11 f. Solaris 10.0,11.0,11.1,11.2,11.3.11.4 g. Oracle Linux 6,7,8,9 h. AIX 6.1,7.1,7.2 & 7.3 1. SUSE Linux 12,15 j. MacOS BigSur, Monterey, Ventura, Sonoma, Sequoia	We request to remove the EOL declared OS from the specification. The solution must support legacy and rare operating systems including but not limited to the below mentioned operating system: a. Microsoft Windows 10,11, Windows Server 2012 & 2012 R2, 2016,2019, 2022 b. RHEL 6,7,8,9 c. CentOS 6,7,8 d. Ubuntu 16,18,2022 e. Debian 9.10 & 11 f. Oracle Linux 6,7,8,9 g. SUSE Linux 12,15 h. MacOS Monterey, Ventura, Sonoma, Sequoia	Tender Conditions Prevail. No Change
357	End point. Detection & Response>SI.No. 37 page 156	Must have a host-based intrusion prevention system (HIPS) to virtually patch known and unknown vulnerabilities before a patch is available or deployable.	We request to remove this specification.	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:49:51 +05'30'

358	220 and	SIEM and SOAR Integration Only Existing EDR Endpoints 1303ntegration of existing EDR server with SIEM/SOAR, security event correlation, alerting, and incident analysis. No EDR deployment or licensing applicable	Please confirm when will the existing EDR contract end. Please confirm whether these 1303 endpoints are included the 6000 EDR as requirement	Please refer Clause 31 in Page No. 109, 110 of the Tender Document
359	Project timeline	Project timeline	Expected project duration, phase-wise rollout vs full rollout, and pilot environment requirements	Please refer Clause 8 in page no.17of the tender document
360	218 and table 2	Service Edge(SSE)/Proxy Gateway	Please share the sizing details and specification for the SSE solution	Shall be sized based on the number of users as per Scope of Coverage Section in page no. 125 of Tender Document.
361	Cyber Security Operation Centre Bill of Quantities	Antiphishing	No of Mailbox	Shall be sized based on the number of users as per Scope of Coverage Section in page no. 125 of Tender Document.
362	Cyber Security Operation Centre Bill of Quantities	Discom	No of Discoms	It is to clarify that Discom means “BESCOM” – 1 no.
363	ITSM	ITSM	No of Asssets & Agents/Technicians required	Tender Conditions Prevail. No Change
364	Page 218	WAF Application	License Required/throughpout/No of applicatios	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:50:34 +05'30'

365	Page 218	DDoS Protection	No of applications to be protected & Throughout License required.	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
366	Page 218	Unified Endpoint Management (UEM)	No of end points to be monitored/Managed	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
367	Page 218	PAM	No of Privileged accounts	As per the Scope coverage in Tender document.
368	Page 218	Licensed for max of 50 Databases or equivalent per Discom including all installation	No of Database to be Monitored.	Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document.
369	55 and 4.4,7	Deploy EDR agents across all enterprise endpoints, servers, and critical OT systems	Request to confirm the total number of critical OT endpoint system	Approx. 250 nos. of critical OT endpoint system
370	Page 55	Number of databases to be monitored	Please provide total database count and types (Oracle, SQL Server, MySQL, PostgreSQL, etc.	Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document.
371	Page 55	Database deployment environment	Clarify on-prem vs cloud deployment, and total number of database servers/instances	All solutions shall be strictly on premises. Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document.
372	Page 55	Transaction volume	Approximate daily transaction volume (TPS) and log volume (GB/day) for sizing purposes	Please refer Technical Specification 1. SIEM, Sl no. 08, in Page no. 127 of the tender document for sizing

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:51:23 +05'30'

373	Page 55	Privileged accounts	Number of DBA and service accounts to be monitored.	Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document.
374	Page 55	Licensing metric	Confirm licensing metric per DB server, per core, per instance, or per appliance	Please refer Section 7, Clause 2. Payment Schedule, Table-2 in page no. 219 of the Tender document.
375	Page 55	Retention & storage	Expected log retention period and storage sizing requirements	Please refer Clause no 16 & 17 in Page no 83-87 of the tender document.
376	Page 55-56	High Availability / DR	Confirm if HA / clustering / DR setup is required	Please refer the note mentioned below in this document
377	Page 55-56	Applications to protect	Total number of mobile applications (Android/iOS) including production, UAT, and dev apps	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
378	Page 55-56	User base	Average monthly active users and expected annual downloads for sizing and license estimation	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document.
379	Page 55-56	Licensing model	Confirm licensing metric - per app, per MAU, per API call or per year subscription	Please refer Section C. Tool AMC in Page no.221of Tender Document.
380	Page 55-56	API coverage	Clarify whether backend API protection is included within RASP licensing	Yes
381	Page 55-56	Dashboard & hosting	Clarify whether monitoring dashboard is SaaS or on-prem, and data residency requirements	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:52:08 +05'30'

382	Page 55-56	SOC integration	Method of alert forwarding to SOC (Syslog/API) and SLA for threat alerting	Please refer clause no 18 in Page No 87,88 of the tender document
383	Page 56-57	Device inventory	Total desktops, laptops, macOS, Linux, Android, and iOS devices to be on boarded	Please refer Section C. Tool AMC in Page no.221of Tender Document. The count is same as EDR.
384	Page 56-57	Device ownership	BYOD vs corporate-owned split and remote workforce percentage	Tender Conditions Prevail. No Change
385	55 and 7	The proposed solution should provide on premises virtual server component which will be hosted at the customer data centre in a forward proxy mode for any communication between endpoints and the OEMs EDR solution	Kindly confirm whether OT network is having connection with the forward proxy to comply connection with OEMs EDR solution as per RFP request	Tender Conditions Prevail. No Change
386	Page 57	PAM	How many numbers of assets needs to be onboarded onto PAM	All endpoint users as covered in clause 31 in page no.109 of Tender Document
387	Page 57	PAM	What are the kind of assets that needs to be integrated to the PAM.	All endpoint users as covered in clause 31 in page no.109 of Tender Document
388	Page 57	PAM	What kind of deployment is BESCOM looking for PAM. For e.g., Standalone, DC-DR, HA in DC-DR etc.	Both in DC & DR

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:53:07 +05'30'

389	Page 57	PAM	What kind of thick client based/exe-based applications used by customer that needs to be on boarded onto PAM. Kindly help with the names of these applications if any.	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document and BOQ section of Tender document.
390	Page 57	PAM	What kind of a deployment is the customer looking for - For instance, on premises/cloud/hybrid	On premises
391	Page 57	SSO and MFA	Please share the indicative list of applications and users to be integrated with SSO (cloud, on prem, custom), along with their authentication capabilities (SAML/OIDC only, form based, etc.)	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document and BOQ section of Tender document.
392	Page 57	SSO and MFA	Please clarify whether SSO is required for internal users only, or also for external users (partners, customers, vendors) and whether CIAM/B2B/B2C use cases are in scope.	This is to clarify that SSO is required for internal users & also for external users
393	Page 57	SSO and MFA	Please specify the mandatory MFA methods (e.g., TOTP app, push notification, FIDO2/WebAuthn security keys, hardware tokens, SMS/email OTP as backup only).	This is to clarify that MFA methods can be TOTP, push notification .

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:53:51 +05'30'

394	Page 57	PAM	How many number of privileged users are you looking for a PAM solution to be implemented	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document and BOQ section of Tender document.
395	Page 56-57	Licensing metric	Confirm licensing model - per device, per user, bundled with E3/E5, or other	Licensing shall be per device.
396	Page 56-57	Security controls	Scope for patch management, encryption (BitLocker/FileVault), remote wipe, DLP, and USB/device control	Tender Condition Prevails. No change
397	Page 56-57	HA / DR requirement	Clarify high availability and disaster recovery requirements for UEM infrastructure	Solution should be in HA mode
398	Page 56-57	SIEM integration	Specify SIEM platform and expected alert forwarding / correlation requirements	Tender Conditions Prevails. No change.
399	Page 218	NBAD	Considered for Licensing of 500Mbps Network traffic per Discom - clarification required	Tender Conditions Prevails. No change.
400	Page 218	V M	No of assets / IPs	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender Document and BOQ section of Tender document.
401	Page 218	Mobile Application Security (RASP)	No of Mobile APP to be protected & Flavours	Please refer Scope of Coverage Section in page no. 124 and 125 of Tender

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:54:36 +05'30'

				Document and BOQ section of Tender document.
402	Page 99	Performance Testing - Demonstration of greater than 99.9 percent availability and less than 3 second response time under peak load.	Need Clarity on this	Please refer Clause no.27 in page no.99 of the tender document.
403	Page 67	The tenderer shall provide emergency support even beyond the contract period (Five years after Go-Live) until BESCOM transitions to a new service provider or in house operations.	Duration not clear. Please clarify	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:55:43 +05'30'

404	Page 212 213 SCC Clause SC2 Liquidated Damages	Liquidated Damages and SLA penalties	We understand that the RFP includes penalty provisions for service level non compliance Considering the long term nature and operational dependency of the project multiple factors including external integrations third party dependencies and customer infrastructure may impact service levels despite best efforts To ensure balanced contractual risk and wider participation we request the authority to kindly cap the overall cumulative penalty under the contract to a maximum of 5 percent of the contract value We request the authority to amend the clause accordingly	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:56:36 +05'30'

405	Page 216 SECTION 7 Payment Terms and Milestones	Payment for One Time Setup Cost	We understand that the RFP defines the payment milestones for one time setup cost as 55 percent on supply 25 percent on installation and commissioning and 20 percent after FAT UAT and 6 months successful operation Considering the significant upfront procurement and implementation cost involved in establishing the solution infrastructure we request the authority to kindly revise the payment terms to 80 10 10 to ensure smoother project execution and cash flow alignment Proposed payment terms 80 percent on supply delivery inspection and acceptance of BoM items 10 percent on successful installation commissioning and readiness certification 10 percent on successful FAT UAT and submission of required reports We request the authority to kindly consider and amend the clause accordingly	Tender Conditions Prevail. No Change
406	PgNo14	SOAR	Proof of Concept Demonstration - SOAR	Tender Conditions Prevail. No Change

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:57:28 +05'30'

407	PgNo 127	Technical Spec - UEBA	Request BESCOM to add the UEBA Technical Specification which is currently missing as apart of the RFP.	UEBA shall be provided as part of SIEM solution.
408	Page 216	Supply and Procurement of Hardware - Part-A Part-B Part-C -55 percent	Supply and Procurement of Hardware - Part-A Part-B Part-C -70 percent	Tender Conditions Prevail. No Change
409	Page 216	Installation Commissioning and SOC Control Room Setup - Part-B Part-C Part D (Licensing charges as per BoQ) - 25 percent	Installation Commissioning and SOC Control Room Setup - Part-B Part-C Part D (Licensing charges as per BoQ) - 20 percent	Tender Conditions Prevail. No Change
410	Page 216	Factory Acceptance Test (FAT) User Acceptance Test (UAT) Post Implementation & SLA Compliance - Part-A Part-B Part-C - 25 percent	Factory Acceptance Test (FAT) User Acceptance Test (UAT) Post Implementation & SLA Compliance - Part-A Part-B Part-C - 20 percent	Tender Conditions Prevail. No Change
411	Technical Scoring Criteria, Page 11, Sl No.6.	The proposed NG-SIEM solution should have been successfully supplied and implemented in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large-scale high demand environments for future expansions as well, supported with PO/Work order/Invoice copy.	-	To be read as: The proposed NG-SIEM solution should have been successfully supplied and implemented in an on premise setups in any one Indian Critical Government Organizations with 25000 EPS in the last 5 years considering the capability to support large-scale high demand environments for future expansions as well, supported with PO/Work

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:58:14 +05'30'

		Supply Experience- Number of references with Events Per Second(EPS): □ No References – 0 Points □ = 1 References– 8 Points □ >= 2 References–10 Points Min Points: 15 Max Points: 30		order/Invoice copy. Supply Experience- Number of references with Events Per Second(EPS): □ No References – 0 Points □ = 1 References– 15 Points □ >= 2 References–30 Points Min Points: 15 Max Points: 30

Note:

The selected bidder shall design, supply, implement, commission, operate and maintain a Centralized Security Operations Centre (CSOC) for Bangalore Electricity Supply Company Limited (BESCOM) in accordance with the architecture and obligations set forth in the clauses below.

1. **Bidder Eligibility**

The bidder, whether an Original Equipment Manufacturer (OEM), System Integrator (SI), or an authorised vendor, shall be eligible to participate in the bidding process, subject to full compliance with the qualification criteria and conditions stipulated in this tender document.

2. On-premise Primary CSOC Setup – BESCOM HSR Data Centre (DC)

1. The complete C-SOC solution stack (SIEM, SOAR, UEBA, NBAD, DAM, TIP, EDR, VM, RASP, EASM, DDoS Protection, WAF, API & Bot Protection, UEM, SSO Integration, Log Management, Incident Management, Forensics) shall be deployed at on

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:59:04 +05'30'

premise BESCOM HSR DC. Ensuring On-premise primary CSOC in DC. CSOC monitoring setup should be planned in corporate office at the provisioned room by Bescom.

2. BESCOM shall provide only rack space at the DC. All required hardware, compute, storage, network components, redundancy, licences, installation and commissioning shall be within the bidder's scope.
3. Integration with BESCOM IT/OT/IoT systems, control centres, corporate office, zonal/divisional offices and all security devices shall be ensured.
4. Logging and event retention shall comply with CERT-In guidelines for the entire duration of the contract.

3. Disaster Recovery (DR) CSOC Setup – MeitY Empanelled Cloud (India)

1. A fully functional DR CSOC shall be established with a Cloud Service Provider (CSP) empanelled under the Ministry of Electronics and Information Technology (MeitY) framework, within India other than DC location Bangalore.
2. Data residency shall be strictly within Indian territory. Under no circumstances shall any data, logs, or configurations be hosted, processed, or transmitted outside India.
3. The DR environment shall not function as a cold backup. The full C-SOC solution stack shall be deployed and maintained in a continuously operational state.
4. Near real-time replication of logs, configurations, incidents, artefacts, dashboards and threat intelligence feeds shall be ensured between the Primary DC and the DR environment.
5. The architecture shall support Active-Standby or Active-Active mode, as proposed by the bidder and approved by BESCOM.
6. Configurable replication factors within the DC and between DC–DR shall be supported and documented.
7. The solution shall ensure near-zero Recovery Point Objective (RPO) and minimal Recovery Time Objective (RTO), with clearly defined and tested failover and failback mechanisms.
8. DR drills shall be conducted at a minimum twice annually, with documented test plans and execution reports submitted to BESCOM within ten (10) working days of each drill.

4. Security, Compliance & Continuity

1. Encryption at rest and in transit, KMS-based key management, Role-Based Access Control (RBAC), audit logging, and log immutability/WORM controls (where applicable) shall be enabled and maintained throughout the contract period.
2. Secure connectivity between the Primary DC and the DR environment shall be established via IPSec VPN, MPLS, or Direct Connect equivalent, with redundant links to ensure uninterrupted replication.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 16:59:55 +05'30'

3. The DR environment shall remain continuously synchronised and updated with all changes applied at the Primary DC.
4. No data loss shall occur during planned or unplanned failover scenarios. Zero data loss is a mandatory contractual obligation.
5. All data, logs and configurations shall remain the sole property of BESCOM and shall not be hosted, replicated or backed up outside Indian territory, nor shall such data be utilised by the bidder for any purpose other than the delivery of contracted services to BESCOM.

5. DR Ownership, Accountability & Governance

The selected bidder shall bear complete and undivided responsibility for the design, implementation, operation and maintenance of the DR environment throughout the entire contract period. This obligation is non-transferable and shall remain in full force, without exception, for the duration of the engagement.

6. Licensing, Subscriptions & Support Management

All software licences, platform subscriptions and associated OEM support and maintenance services required for the delivery of the contracted scope shall be procured, renewed and managed by the bidder entirely at its own cost. The Bill of Quantities (BOQ) submitted by the bidder shall comprehensively cover licence and subscription costs for both the on premise Primary DC and the DR environments.

The bidder shall ensure that all licences and support entitlements remain valid, active and uninterrupted throughout the contract period, including any extensions thereof. Licences shall be renewed by the bidder no later than thirty (30) days prior to their respective expiry dates, and evidence of renewal shall be submitted to BESCOM within five (5) working days of completion.

7. Synchronisation, DR Readiness & Activation

The DR environment shall be maintained in continuous synchronisation with the Primary DC at all times, to preserve data integrity and ensure operational readiness. The bidder shall ensure that the DR environment is capable of assuming full C-SOC operational responsibilities without interruption.

Upon receipt of a formal instruction from BESCOM, or upon the occurrence of a pre-agreed automated trigger condition, the bidder shall activate and sustain all contracted C-SOC services from the DR site without any degradation in monitoring coverage, incident detection or response capability.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 17:00:43 +05'30'

8. **Exit Management & Transition**

1. The bidder shall maintain comprehensive and up-to-date documentation throughout the contract period, covering architecture diagrams, configuration baselines, integration runbooks, use-case catalogues and operational procedures.
2. Upon contract expiry or termination, the bidder shall provide a minimum ninety (90) day transition support period. All data, configurations, credentials and documentation shall be handed over to BESCOM or its nominated successor vendor in a structured, complete and secure manner.
3. All BESCOM data shall be securely and verifiably erased from bidder-owned or bidder-managed infrastructure within thirty (30) days of completed data handover. A Certificate of Data Destruction shall be furnished to BESCOM upon completion by all of its employees involved in C-SOC project with BESCOM.
4. The bidder shall provide structured knowledge transfer to BESCOM's designated staff and any incoming service provider to ensure business continuity with no service disruption during the transition period.

Note: These clauses form an integral part of the Scope of Work and the General Conditions of Contract. The bidder shall incorporate all associated costs — including hardware, cloud hosting, replication, licences, implementation, testing, DR drills, operations and exit/transition support — within the Financial Bid. No separate or additional claims on account of these obligations shall be entertained after award of contract.

All other terms and conditions as specified in the Tender Document remains unaltered.

BENNUR GUTHYAPPA PAKKEERAPPA

Digitally signed by BENNUR GUTHYAPPA PAKKEERAPPA
Date: 2026.03.10 17:01:36 +05'30'